HOPEX IT Risk Management

Benutzerhandbuch

MEGA HOPEX V1R3
1. Ausgabe (Juli 2015)

Die in diesem Dokument enthaltenen Informationen können jederzeit ohne vorherige Ankündigung geändert werden und stellen in keinem Fall eine Verpflichtung für MEGA International dar.

Diese Veröffentlichung darf weder ganz noch teilweise ohne vorherige schriftliche Erlaubnis von MEGA International für irgendwelche Zwecke reproduziert, gespeichert, übersetzt oder übertragen werden, unabhängig davon, mit welchen Mitteln dies geschieht.

© MEGA International, Paris, 1996 - 2015

Alle Rechte vorbehalten.

HOPEX Internal Control und MEGA sind eingetragene Marken von MEGA International.

Windows ist eine registrierte Marke von Microsoft.

Die anderen Marken gehören den jeweiligen Eigentümern.

INHALT

Inhalt 3

Einführung 11

Die Lösung 12
Management der IT-Risiken 12
Management der IT-Compliance 12
Management der IT-Anbieter. 12
Über dieses Handbuch 13
Struktur des Handbuchs 14
Weitere Ressourcen 14
Schreibkonventionen in diesem Handbuch 15
Konvention zur Formulierung der Befehle 15

Der Desktop HOPEX IT Risk Management 17

Verbindung zu HOPEX IT Risk Management. 19
Grundvoraussetzungen 19
Dateien zur Nutzung von HOPEX IT Risk Management importieren. 19
Anwendung starten 20
Präsentation der Benutzeroberfläche. 23
Die Geschäftsrollen HOPEX IT Risk Management 24
Geschäftsanalyse der TransformationHOPEX IT Risk Management 24
Funktionaler Administrator IT RM. 24
IT RM Manager 24
Eigentümer einer Anwendung 25

Überblick über die Rechte nach Geschäftsrolle 25
Rechte hinsichtlich IT-Risiken *25*

Umgebung der Lösungen MEGA 27

Die Bibliotheken 28
Die Organisation 29
Die Prozesse 30
Die Prozesstypen *30*
Die Merkmale eines Prozesses *30*
Die Entitäten 32
Zugriff auf die Entitäten der Organisation *32*
Entität erstellen *33*
Die Geschäftssparten der Organisation 34
Zugriff auf die Geschäftssparten *34*
Umfang der Geschäftssparten *35*
Risiken und Kontrollen 36
Die Risiken 36
Risikofaktoren *39*
Risikofolgen *39*
Die Kontrollen 40
Der Umfang einer Kontrolle *41*
Die Kontrolltypen *41*
Umgebung der Vorschriften 43
Die Vorschriften 43
Zugriff auf die Vorschriften der Organisation *43*
Merkmale einer Vorschrift *43*
Ziele und Anforderungen 45
Auf Ziele und Anforderungen zugreifen *45*
Merkmale der Ziele *45*
Merkmale der Anforderungen *46*
Finanzdaten 48
Die Produkte 48
Die Finanzkonten 49
Ressourcen des Unternehmens 50
Die Anwendungen 50
Datenbanken und Server 52
RACI 53
Verantwortungsstufen *53*
Verantwortungen angeben *53*

Bibliothek verwenden 55

Bestand der IT-Assets 56
Über den Bestand der IT-Assets 56
Bestand des IT-Assets aufstellen *56*

Typen von IT-Assets *56*
Anwendungen beschreiben 57
Allgemeine Merkmale der Anwendung *57*
Anwendungstyp *57*
Funktionaler Umfang der Anwendung *57*
Verantwortungen hinsichtlich einer Anwendung *58*
Mit den Anwendungen verbundene Technologien *58*
Ausgetauschte Daten *58*
Anfälligkeiten einer Anwendung *59*
Mit einer Anwendung verbundene Kontrollen *59*
Softwareinstallationen *59*
Technologien beschreiben 59
Zugriff auf die Techologien *59*
Merkmale einer Technologie definieren *60*
Technologietypen *60*
Risiken und Anfälligkeiten einer Technologie *60*
Bestand der Bedrohungen und Anfälligkeiten 61
Beispiele von Bedrohungen, Anfälligkeitstypen und Anfälligkeiten 61
Alle Bedrohungen 61
Zugriff auf Bedrohungen *61*
Bedrohungstyp erstellen *62*
Merkmale der Bedrohungen *62*
Anfälligkeiten aufrufen 62
Zugriff auf Anfälligkeiten *62*
Anfälligkeitstyp erstellen *62*
Merkmale der Anfälligkeiten *63*
Umfang der Anfälligkeiten *64*
CVSS-Bewertung *64*
Berichte über die Anfälligkeiten *65*
Bestand der Risiken und Kontrollen 66
Risiken aufrufen 66
Zugriff auf die Risiken *66*
Bewertete Merkmale *66*
Umfang des Risikos *67*
Analyse des Risikos *67*
Bewertung des Risikos *67*
Bearbeitung des Risikos *67*
Kontrollen aufrufen 68
Zugriff auf die Kontrollen *68*
Umfang einer Kontrolle *68*
Bewertung der Kontrollen *68*
Arbeitsumgebung für Fragebögen vorbereiten 68
Bestand der Anforderungen und Vorschriften 69
Merkmale der Vorschriften *69*
Merkmale von Anforderungen *69*
Bestand der Anbieter 70
Zugriff auf die Liste der Anbieter *70*
Merkmale der Anbieter *70*
Liste der angebotenen Technologien *70*
Bewertung des Anbieterrisikos *70*

HOPEX IT Risk Management benutzen 71

IT-Risiken verwalten. 72
IT- und Softwarebestand aufstellen. 72
Anfälligkeiten auf IT-Assets positionieren. 72
Risiken identifizieren 73
Risiken auf IT-Assets positionieren 73
Risiken über eine Kreuztabelle positionieren 73
Risiken einzeln auf jedes Asset positionieren 73
Risikoszenarios identifizieren 74
Risikoszenario erstellen 74
Diagramm über Risikoszenario erstellen 74
Bericht über die Risikoursache 76
Beispiele: 77
So genannte Experten-Risiken bewerten 78
Direkte Bewertung von Risiken. 78
Bewertungsvorlagen der Risiken. 79
Aktionspläne für eine Verbesserung beschreiben. 79
IT-Compliance verwalten 80
Bestand der Kontrollen und Kontrolltypen aufstellen 80
Verbindungen zwischen Kontrollen und Kontrolltypen 80
Kontrolltypen mit vorschriftsmäßigen Anforderungen verbinden 81
Umfang der Anwendungen einer Kontrolle 81
Vorschriftsmäßige Anforderungen definieren 81
Kontrollen der Anwendungen identifizieren. 82
Kontrollen von Experten bewerten 82
Kontrollen direkt bewerten 82
Vorlage für die Bewertung der Kontrollen 83
IT-Anbieter verwalten. 84
IT-Anbieter identifizieren 84
Kosten von Produkten und Services angeben 84
Anbieter bewerten 85

Bewertungen mit Fragebögen 87

Prinzip der Bewertung mit Kampagnen 88
Präsentation der Konzepte 88
Bewertungssitzung 88
Fragebogen 88
Bewertungskampagne. 88
Etappen der Bewertung 88
Arbeitsumgebung vorbereiten 88
Kampagne und Bewertungssitzungen starten. 89
Bewertungssitzung erstellen 91
Zugriff auf Bewertungskampagnen 91
Bewertungskampagne erstellen 91
Bewertungssitzung erstellen 92
Zugriff auf Bewertungssitzungen. 92

Bewertungssitzung erstellen 92
Vorschau der Parameter der Bewertungssitzung 92
Sitzungen in einer Kampagne planen (optional) 94
Bewertungskampagne bereitstellen 94
Umfang der Bewertungskampagne und Beantworter definieren 95
Umfang der Bewertungskampagne definieren 95
Beantworter angeben 95
Bewertungen innerhalb verschiedener Sitzungen aufteilen 95
Bewertungskampagne freigeben 97
zu bewertende Objekte und ihre Kontexte anzeigen 98
Umfang der Sitzung und Beantworter definieren 99
Umfang der Sitzung definieren 99
Beantworter angeben 99
Zu bewertende Objekte und ihren Kontext freigeben 100
Bewertungssitzung freigeben 100
Generierte Fragebögen anzeigen 100
Fragebögen neu generieren 101
Fragebögen senden 102
Fragebögen ausfüllen 103
Zugriff auf Bewertungsfragebögen 103
Übertragung eines Fragebogens beantragen 103
Fortschritt der Fragebögen verfolgen 105
Ergebnis der Sitzung aufrufen 105
Gesendete Fragebögen anzeigen 105
Bewertungsfragebögen freigeben 105
Beantworter auffordern, seine Antworten zu ändern 105
Fragebogen neu zuweisen 106
Bewertungssitzung schließen 108

Risiken identifizieren 109

Modus der Risikobearbeitung 110
Bearbeitungsmodi 110
Risikostufen 111
Umzusetzende Kontrollen und Aktionen angeben 111
Aktionspläne verwalten 113
Aktionsplan erstellen 113
Aktionsplan charakterisieren 113
Allgemeine Merkmale 114
Finanzanalyse 114
RACI 115
Erfolgsfaktoren 115
Umfang 115
Meilensteine 115
Anlagen 115
Aktionen verwalten 115
Workflows der Aktionspläne 116
"Bottom-up"-Methode 116

"Top-down"-Methode *117*
Workflow der Aktionen *117*
Folgemaßnahmen bei Aktionsplänen 117
Fortschritt eines Aktionsplans angeben *117*
Berichte über Folgemaßnahmen der Aktionspläne *117*

Berichte in HOPEX IT Risk Management 121

Zugriff auf Berichte 122
Zugriff auf die Registerkarte der Berichte *122*
Zugriff auf Berichte, die direkt bei den Objekten verfügbar sind *122*
Zugriff auf Widgets *122*
Berichte über IT-Risiken 124
Berichte über IT-Risiken 124
Kritizität der Anwendungen *124*
Tabelle Bedrohungen und Anfälligkeiten *125*
Berichte über IT-Assets 126
Aggregierte Risikostufe nach Geschäftsprozess *126*
Heatmaps der Risiken *127*
Heatmap der Anwendungen *129*
Widgets für Risiken *130*
Bericht über die Risikoursache *132*
Berichte über die Anfälligkeiten 132
Berichte über IT-Compliance 135
Identifizierung der Kontrollen 135
Pfad *135*
Parameter *136*
Ergebnis *136*
Beispiel *136*
Kontrollstufe nach Vorschrift 137
Pfad *137*
Parameter *138*
Ergebnis *138*
Beispiel *139*
Kontrollstufe nach Geschäftsprozess 139
Pfad *139*
Parameter *139*
Ergebnis *139*
Beispiel *140*
Widgets für Compliance 140
Compliance der Prozesse *141*
Regulatorische Compliance *141*
Globale Kontrollstufe *142*
Bericht über die Verwaltung der Anbieter 144
Kreuztabelle Anbieter nach Typ X Risikostufe 144
Pfad *144*
Parameter *144*
Ergebnisse *144*
Beispiel *144*

Risikostufe Anbieter nach Geschäftssparte 145
Pfad *145*
Parameter *145*
Ergebnisse *145*
Beispiel *145*
Berichte über die Bewertungen 146
Folgemaßnahmen - Sitzungen 146
Pfad *146*
Parameter *146*
Ergebnis *146*
Sitzungsstatistiken 146
Pfad *147*
Parameter *147*
Ergebnis *147*

Glossar 149

Anhang - Workflows 157

Workflow von Bewertungen 158
Generischer Workflow einer Bewertungskampagne 158
Generischer Workflow einer Bewertungssitzung 159
Generischer Workflow der Fragebögen 159
Workflows der Aktionspläne 161
Workflow des Aktionsplans "Top-down" *161*
Workflow des Aktionsplans "Bottom-up" *162*
Workflow einer Aktion *163*

Index 165

EINFÜHRUNG

Jedes Unternehmen muss Governance-Prozesse und Prozesse Im Rahmen des IT-Managements einrichten.

HOPEX IT Risk Management ermöglicht, das richtige Governance-System zu definieren und zu automatisieren. Mit dieser Lösung können Risiken ab der aktuellen IT-Architektur analysiert und die notwendige Kontrollstufe definiert werden, um die Ziele des Unternehmens zu erreichen. **MEGA** erstellt vor allem eine adäquate Kontrollumgebung, die die Prozesse des Unternehmens unterstützen.

Die Lösung richtet sich an die IT-Abteilungen und vor allem an die Abteilungen, die für das Management von Risikos, Compliance und der IT-Sicherheit zuständig sind.

- ✓ "Die Lösung", Seite 12
- ✓ "Über dieses Handbuch", Seite 13
- ✓ "Schreibkonventionen in diesem Handbuch", Seite 15

Die Lösung

HOPEX IT Risk Management ermöglicht, Risiken, Compliance und IT-Anbieter zu verwalten. Sie können die von **MEGA Architecture** oder **MEGA IT Portfolio Management** vererbten Bestände nutzen oder sie direkt in der Lösung erfassen.

Management der IT-Risiken

HOPEX IT Risk Management ermöglicht:

- Bedrohungen und Anfälligkeiten identifizieren, wobei entsprechende Frameworks und Informationsquellen als Grundlage dienen (zum Beispiel: ISO 27005, CVE).
- Berichte über die Anfälligkeiten zu generieren und Risiken zu identifizieren, die IT-Assets gefährden.
- Die Risikostufe der IT-Assets mit einem so genannten Experten zu bewerten, oder anhand von Fragebögen, die an die Eigentümer einer Anwendung gesendet werden.
- Risikoszenarios und die Verbindungen von Ursache und Wirkung zwischen den Risiken zu identifizieren.

Management der IT-Compliance

IT-Abteilungen müssen sich an eine Reihe von vorschriftsmäßigen Anforderungen richten und dementsprechend für IT-Assets verschiedene Kontrollen durchführen.

HOPEX IT Risk Management ermöglicht:

- die angemessenen IT-Regelwerke (ISO 27002, NIST), die daraus entstehenden Anforderungen und die Typen der durchzuführenden Kontrollen zu identifizieren.
- die Kontrollstufe (Design und Effizienz der Kontrolle) mit einem so genannten Experten zu bewerten, oder anhand von Fragebögen, die an die Eigentümer einer Anwendung gesendet werden.
- Berichte zu generieren, in denen die erreichte regulatorische Compliance-Stufe veranschaulicht wird.

Management der IT-Anbieter

HOPEX IT Risk Management ermöglicht:

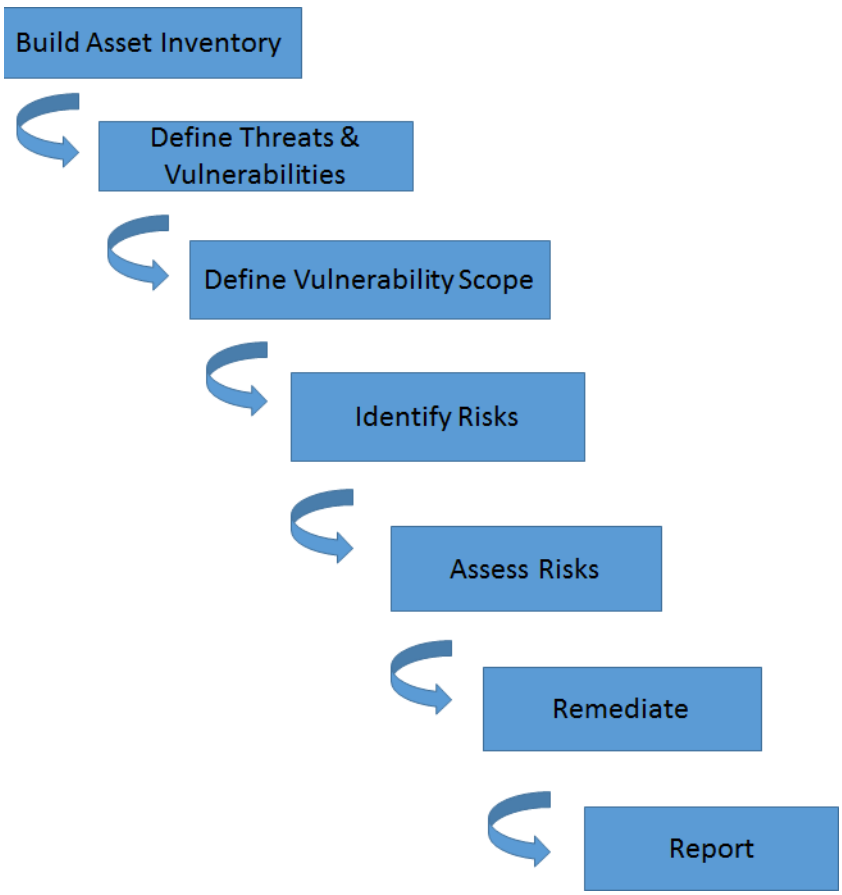
- Verkaufsdaten des Anbieters einzugeben
- Bewertungskampagnen zu starten, um die Beziehung mit diesen Anbietern zu bewerten
- die globale Risikostufe des Anbieters zu bewerten

ÜBER DIESES HANDBUCH

Dieses Handbuch präsentiert die Funktionalitäten der Lösung HOPEX IT Risk Management. Das Handbuch erklärt folgenden Etappen:

- Bestand des IT-Assets aufstellen
- Bedrohungen und Anfälligkeiten definieren
- Risiken identifizieren
- Risiken bewerten
- Risiken bearbeiten
- Reporting

> ☛ *Die Reporting-Funktionalitäten können jederzeit global oder für die Etappen eines Prozesses jeweils einzeln aufgerufen werden.*



Struktur des Handbuchs

Das Handbuch setzt sich aus folgenden Kapiteln zusammen:

- ✓ "Umgebung der Lösungen MEGA", Seite 27, beschreibt die verschiedene Elemente der Umgebung, die in den Lösungen **MEGA**verwendet werden.
- ✓ "Bibliothek verwenden", Seite 55, beschreibt den Bestand des IT-Assets, der Bedrohungen und Anfälligkeiten, Risiken und Kontrollen, Anbieter.
- ✓ "HOPEX IT Risk Management benutzen", Seite 71, beschreibt die verschiedenen Use Cases der Lösungen, d. h. das Management von IT-Risiken, Compliance und Anbietern.
- ✓ "Bewertungen mit Fragebögen", Seite 87, beschreibt die notwendigen Schritte zum Versenden von Fragebögen im Rahmen von Bewertungskampagnen.
- ✓ "Risiken identifizieren", Seite 109, beschreibt, wie Risiken bearbeitet und Aktionspläne verwaltet werden.
- ✓ "Glossar", Seite 149
- ✓ "Anhang - Workflows", Seite 157

Weitere Ressourcen

Dieses Handbuch wird ergänzt durch:

- das Handbuch **MEGA Common Features**, das die Benutzeroberfläche von MEGA beschreibt.

  ☛ *Es kann nützlich sein, dieses Handbuch aufzurufen, um eine allgemeine Darstellung der Benutzeroberfläche zu erhalten.*

- das Administrationshandbuch MEGA Administration - Supervisor.

SCHREIBKONVENTIONEN IN DIESEM HANDBUCH

☛ *Anmerkung zu den vorherigen Punkten.*
📖 *Definition der verwendeten Begriffe.*
☺ *Tipp, der dem Benutzer das Leben erleichtern kann.*
Kompatibilität mit vorherigen Versionen.
Zu vermeiden.

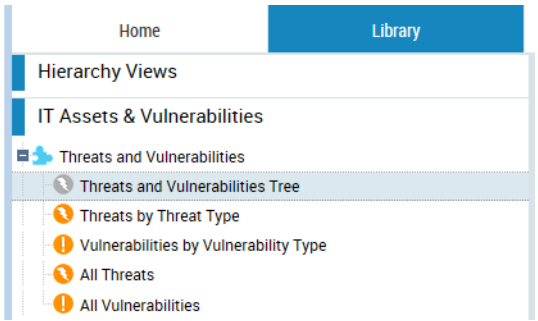
Wichtiger Hinweis zur Vermeidung von Bedienungsfehlern.

Befehle werden wie folgt dargestellt: **Datei > Öffnen**.

Namen von Produkten und technischen Modulen werden wie folgt dargestellt: **MEGA**.

Konvention zur Formulierung der Befehle

Um auf einen Befehl der Lösung zu verweisen wird in diesem Handbuch der Einfachheit halber folgende Formulierung verwendet:

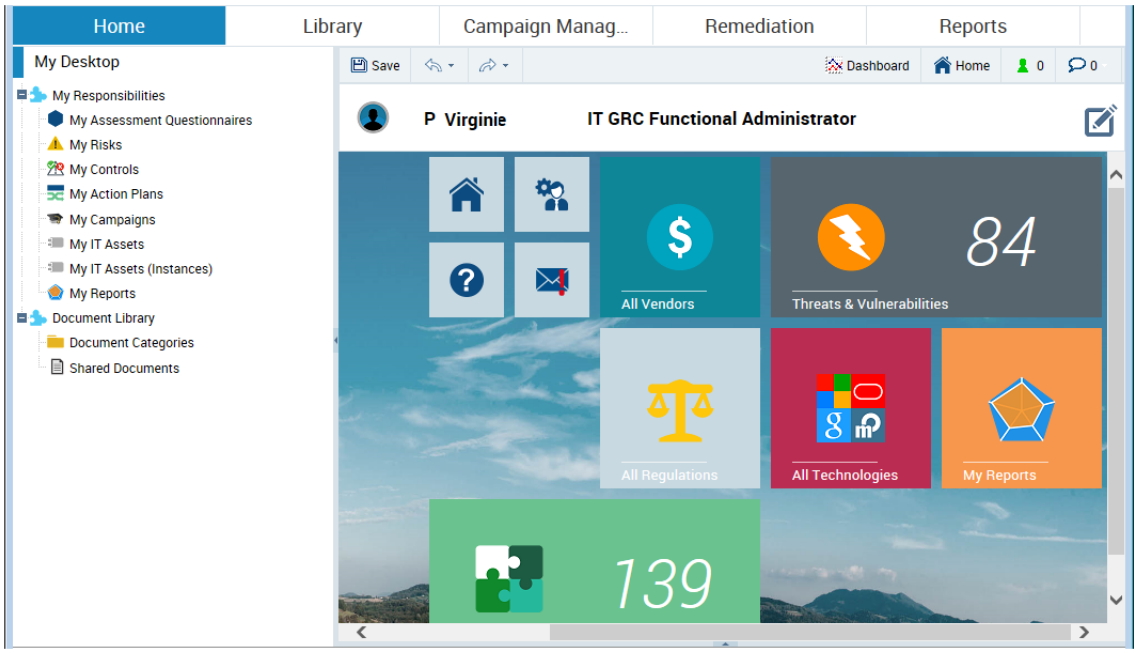
Befehl der Anwendung	Formulierung im Handbuch
	Klicken Sie auf **Bibliothek > IT Assets & Anfälligkeitens > Bedrohungen und Anfälligkeiten > Baumstruktur der Bedrohungen und Anfälligkeiten**.

Beispiel eines Befehls mit Formulierung im Handbuch

DER DESKTOP HOPEX IT RISK MANAGEMENT

Dieses Kapitel macht Sie mit **HOPEX IT Risk Management** vertraut und stellt die einzelnen Schritte vor, die vor Nutzung der Lösung durchzuführen sind.

Zudem werden die verschiedenen Geschäftsrollen präsentiert, die in der Lösung verwendet werden, sowie die entsprechenden verknüpften Rechte.



✓ "Verbindung zu HOPEX IT Risk Management", Seite 19
✓ "Präsentation der Benutzeroberfläche", Seite 23
✓ "Die Geschäftsrollen HOPEX IT Risk Management", Seite 24

VERBINDUNG ZU HOPEX IT RISK MANAGEMENT

✓ "Grundvoraussetzungen", Seite 19
✓ "Anwendung starten", Seite 20

Grundvoraussetzungen

Die **MEGA**-Suite ist installiert.

Um auf die **HOPEX IT Risk Management**-spezifischen Funktionen zuzugreifen, die in diesem Handbuch beschrieben werden, müssen Sie sicherstellen, dass der Administrator folgende Prozeduren durchgeführt hat.

Importe vorbereiten

Die zu importierenden Dateien werden als komprimierte Dateien mitgeliefert, die dekomprimiert werden müssen, bevor sie in ein Repository importiert werden.

Um die **HOPEX IT Risk Management**-spezifischen Dateien zu dekomprimieren, gehen Sie wie folgt vor:

1. Öffnen Sie im Ordner, in dem **MEGA** installiert wurde, den Ordner **Dienstprogramme** und anschließend den Ordner **Solutions Pack**.
2. Doppelklicken Sie auf die Datei **ITGRC.exe**.
3. Klicken Sie in dem nun geöffneten Dialogfenster auf **Extrahieren**.
   Das System erstellt zwei neue Ordner:
   - **ITGRC - Sample**
   - **ITGRC - Technical data**

Dateien zur Nutzung von HOPEX IT Risk Management importieren

Um **HOPEX IT Risk Management**-spezifische Objekte zu importieren, gehen Sie wie folgt vor:

1. Starten Sie "Administration.exe" und verbinden Sie sich mit einem Benutzer, der über die Administrationsberechtigung für Daten verfügt.
2. Erstellen Sie eine neue Umgebung.
3. Verbinden Sie sich mit dieser Umgebung und erstellen Sie ein neues Repository.
4. Klicken Sie mit der rechten Maustaste auf das Repository und wählen Sie **Verwaltung der Objekte > Solution Pack importieren** aus.
   Dann wird das Fenster zur Auswahl eines "Makros" angezeigt.
5. Wählen Sie **ITGRC - Technical data** aus und klicken Sie auf **OK**.
   Sie haben jetzt ein leeres Repository erstellt.
6. Beenden Sie die Anwendung Administration.

Beispielbibliothek importieren

Wenn Sie ein Repository mit einem Beispiel verwenden möchten, gehen Sie wie folgt vor:

1. Führen Sie die Prozedur zum Import aus, die im Absatz "Dateien zur Nutzung von HOPEX IT Risk Management importieren", Seite 19 beschrieben wird.
2. Klicken Sie mit der rechten Maustaste auf das Repository, in das das Beispiel importiert werden soll, und wählen Sie **Verwaltung der Objekte > Solution Pack importieren** aus.
   Dann wird das Fenster zur Auswahl eines "Makros" angezeigt.
3. Wählen Sie **IT GRC - Sample** aus und klicken Sie auf **OK**.
   Sie haben nun ein Repository erstellt, in dem die Beispieldaten enthalten sind.
4. Beenden Sie die Anwendung Administration.

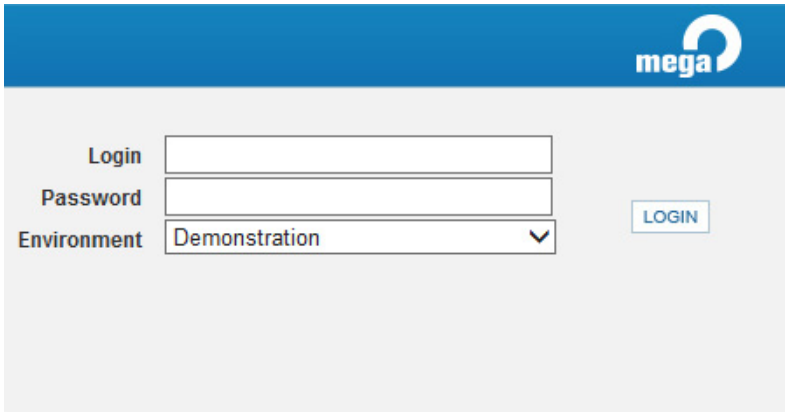
Anwendung starten

Um sich mit einer **MEGA** -Anwendung im Web zu verbinden, gehen Sie wie folgt vor:

1. Starten Sie die Anwendung **MEGA** unter ihrer HTTP-Adresse.

   ☛ *Wenn Sie die Adresse nicht kennen, wenden Sie sich an Ihren Administrator.*

   Daraufhin wird die Verbindungsseite geöffnet.



2. Geben Sie auf der Verbindungsseite im Feld **Login** Ihre ID ein.
3. (Wenn Sie ein Kennwort besitzen) Geben Sie im Feld **Password** Ihr Kennwort ein.

   ☛ *Wenn Sie Ihr Kennwort vergessen haben, klicken Sie auf* Lost password *(unter dem Verbindungsfenster).*

4. Klicken Sie im Feld **Environment** auf den Pfeil und wählen Sie die Arbeitsumgebung aus.

   ☛ *Sollten Sie keinen Zugriff auf eine Umgebung haben, wird die Umgebung automatisch berücksichtigt. Das Feld zur Auswahl der Umgebung wird nicht angezeigt.*

5. Klicken Sie auf **LOGIN**.
   Wenn Sie authentifiziert wurden, wird ein neues Fenster angezeigt.
6. Klicken Sie im Feld **Repository** auf den Pfeil und wählen Sie das Arbeits-Repository aus.

   ☛ *Wenn Sie nur Zugriff auf ein Repository haben, wird dieses Repository automatisch berücksichtigt.*

7. Klicken Sie im Feld **Business Role** oder **Profile** auf den Pfeil und wählen Sie die Geschäftsrolle oder das Profil aus, mit der bzw. dem Sie arbeiten möchten.

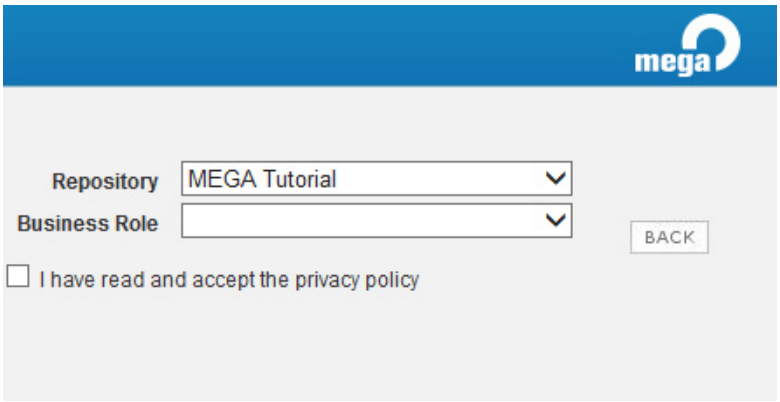
   ☛ *Wenn Sie nur eine Rolle oder ein Profil haben, wird diese Rolle bzw. dieses Profil automatisch berücksichtigt.*

   ☛ *In **MEGA Administration** wird das Feld **Profile** statt **Business Role** angezeigt, wenn in den Optionen der Umgebung (Optionen/ Installation/Benutzerverwaltung) die Option "Verwaltung der Zuweisung von Geschäftsrollen an Personen" nicht ausgewählt wurde.*

   ☛ *Das ausgewählte Profil bzw. die Geschäftsrolle definiert die Anwendungen, auf die Sie zugreifen können.*

8. Klicken Sie im Feld **Application** auf den Pfeil und wählen Sie die Anwendung aus, mit der Sie sich verbinden möchten.

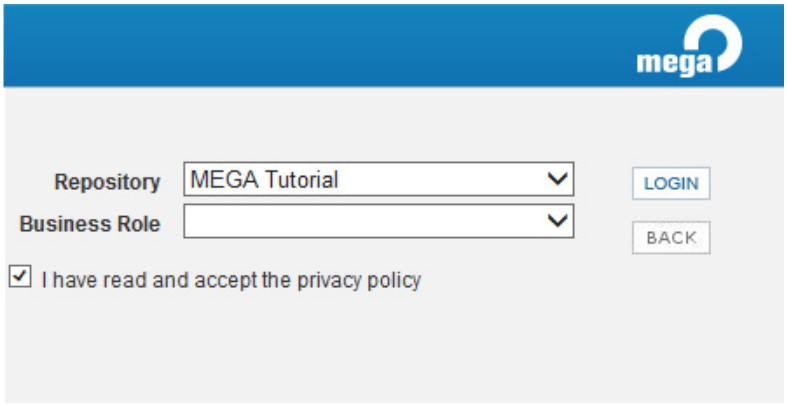
   ☛ *Sollten Sie Zugriff nur auf eine Anwendung mit dem ausgewählten Profil bzw. der Geschäftsrolle haben, wird das Profil/die Rolle automatisch berücksichtigt. Das Feld zur Auswahl der Anwendung wird nicht angezeigt.*



9. Klicken Sie auf Privacy Policy (unter dem Fenster zur Anmeldung) und lesen Sie die Vorschriften hinsichtlich der Datenschutzpolitik durch. Wählen Sie anschließend **I have read and accept the privacy policy** aus.
   Die Schaltfläche **LOGIN** wird angezeigt.

   ☛ *Wenn Sie die Vorschriften hinsichtlich der Datenschutzpolitik gelesen und akzeptiert haben, wird automatisch ein Zertifikat mit Ihrer*

Person verbunden. Zu diesem Schritt werden Sie später nicht mehr aufgefordert.



10. Klicken Sie auf **LOGIN**.

☛ *Klicken Sie auf **BACK**, wenn Sie zum Authentifizierungsfenster zurückkehren möchten.*

Die Home-Page der Web-Anwendung wird angezeigt und eine Sitzung wird geöffnet.

Die angezeigte Seite hängt von der Geschäftsrolle ab, mit der Sie verbunden sind.

☛ *Weitere Informationen zu den verfügbaren Geschäftsrollen finden Sie unter "Geschäftsrollen", Seite 16*

PRÄSENTATION DER BENUTZEROBERFLÄCHE

Die Menüs und Befehle in der Lösung **HOPEX IT Risk Management** hängen von der Geschäftsrolle ab, mit der Sie verbunden sind.

> ☛ *Weitere Informationen zu den Geschäftsrollen finden Sie unter "Geschäftsrollen", Seite 16*

Die Navigationsregisterkarten oben auf der Seite entsprechen den verschiedenen IT-Risiko-Management-Phasen:

- **Bibliothek**
  Siehe "Bibliothek verwenden", Seite 55.
- **Bewertungskampagnen**
  Siehe "Bewertungen mit Fragebögen", Seite 87.
- **Bearbeitung**
  Siehe "Risiken identifizieren", Seite 109.
- **Berichte**
  Siehe "Berichte in HOPEX IT Risk Management", Seite 121.

In der Registerkarte **Home** können Sie auf Objekte zugreifen, für die Sie verantwortlich sind.

Mit einem Dashboard aus Widgets können Sie auf die Synthese von Informationen zugreifen, die im Repository enthalten sind. Weitere Informationen finden Sie unter "Zugriff auf Widgets", Seite 122.

> ☛ *Weitere Informationen zur allgemeinen Verwendung der Benutzeroberfläche finden Sie unter **MEGA Common Features**.*

DIE GESCHÄFTSROLLEN HOPEX IT RISK MANAGEMENT

In **HOPEX IT Risk Management**, gibt es standardmäßig Geschäftsrollen, denen bestimmte Tätigkeiten zugewiesen sind.

☛ *Die Benutzeroberfläche hängt von der Geschäftsrolle ab, die der Benutzer bei seiner Verbindung zur Anwendung ausgewählt hat: die Baumstruktur der Menüs und die Funktionalitäten stellen sich je nach Geschäftsrolle anders dar.*

Geschäftsanalyse der TransformationHOPEX IT Risk Management

Funktionaler Administrator IT RM

Der funktionale IT RM-Administrator (IT Risk Management) verwaltet in erster Linie die Objekte der Umgebung (Organisation, Prozess, Geschäftsfähigkeit, Geschäftssparte und Bestand des IT-Assets).

☛ *Der Anwendungsbestand kann auch zuvor mit **MEGA Architecture** oder **MEGA IT Portfolio Management** von den Application Portfolio und Anwendungsmanagern gebildet werden.*

Er kann auf folgende Desktops zugreifen:

- **Administration**

  ☛ *Weitere Informationen zu diesem Desktop finden Sie im Handbuch **MEGA Administration - Supervisor,** Kapitel "Accessing MEGA Administration".*

- **Umgebung**

  ☛ *Ausführliche Informationen finden Sie unter "Umgebung der Lösungen MEGA", Seite 27.*

- **IT RM**

  ☛ *Weitere Informationen finden Sie unter "Der Desktop HOPEX IT Risk Management", Seite 17.*

Er hat folgende Hauptaufgaben:

- Anwendungsbestand aufstellen
- Bestand der Dienstleister und Softwareunternehmen aufstellen
- jede Anwendung einem oder mehreren IT RM Managern zuweisen
- eventuell Prozessen und/oder Geschäftssparten Anwendungen zuweisen

IT RM Manager

Der IT RM Manager (IT Risk Management) sind die Hauptnutzer der Lösung **HOPEX IT Risk Management**.

Er kann mehreren Abteilungen (Sicherheit, Compliance, Risikomanagement) angehören und

besitzen alle Rechte bezüglich Bedrohungen, Anfälligkeiten, Risiken, Kontrollen, Bewertungsobjekte, Vorschriften, Anforderungen und Berichte.

Er hat folgende Hauptaufgaben:

- Bestand der Bedrohungen und Anfälligkeit aufstellen
- Anfälligkeit jedes Assets identifizieren
- Risiken bei IT-Assets positionieren
- Risiken bewerten
- Aktions- und Verbesserungspläne beschreiben

- Vorschriftsmäßige Anforderungen identifizieren
- Kontrollen identifizieren
- Kontrollen bewerten
- regulatorische Compliance bewerten

- jährliche Kosten der Produkte und Services nach Anbieter erfassen
- Anbieter bewerten

Eigentümer einer Anwendung

Der Eigentümer einer Anwendung beantwortet die Fragebögen, die er im Rahmen von Bewertungskampagnen erhält.

Er kann zudem Aktionspläne übernehmen, die ihm anvertraut wurden.

Überblick über die Rechte nach Geschäftsrolle

Rechte hinsichtlich IT-Risiken

Weitere Informationen finden Sie unter "IT-Risiken verwalten", Seite 72.

	Funktionaler Administrator IT RM	**IT RM Manager**
Anwendungsbestand aufstellen Siehe "Bestand der IT-Assets", Seite 56.	X	
Bestand der Bedrohungen und Anfälligkeit aufstellen Siehe "Bestand der Bedrohungen und Anfälligkeiten", Seite 61.	X	X
Anfälligkeit jedes Assets identifizieren Siehe "Anfälligkeiten auf IT-Assets positionieren", Seite 72.	X	X

	Funktionaler Administrator IT RM	IT RM Manager
Risiken im Zusammenhang mit IT-Assets identifizieren und bewerten Siehe "Risiken identifizieren", Seite 73, "So genannte Experten-Risiken bewerten", Seite 78.	X	X
Risikoszenarios identifizieren Siehe "Risikoszenarios identifizieren", Seite 74.	X	X
Aktionspläne für eine Verbesserung beschreiben Siehe "Risiken identifizieren", Seite 109.	X	X

UMGEBUNG DER LÖSUNGEN MEGA

In diesem Kapitel wird erklärt, wie die in folgenden **MEGA** -Lösungen verwendete Umgebung beschrieben wird: **HOPEX ERM**, **MEGA LDC**, **HOPEX Internal Audit**, **HOPEX Internal Control, HOPEX Regulatory Compliance, HOPEX IT Risk Management.**

☛ *In allen Lösungen werden bestimmte Objekttypen der Umgebung oder Merkmale nicht zwangsläufig verwendet.*

Die **Umgebung** strukturiert, wie die Risiken von allen Mitarbeitern erfasst und berücksichtigt werden, und vor allem das Konzept des Managements und seine Risikobereitschaft, sowie die Umgebung, in der die Organisation tätig ist. Bei diesem Schritt können folgende Punkte aufgestellt werden:

- ✓ eine Bestandsaufnahme über die existierenden Bestände des Unternehmens (Prozesse, Entitäten, Kontrollsysteme, Verantwortlichkeiten, Anwendungen)
- ✓ die Liste der strategischen Ziele, der Organisation und die entsprechenden Anforderungen
- ✓ die internen Umgebungsdaten für das Risk Management

Die Elemente, die mit dem Desktop **Umgebung** verbunden sind, bieten allen Benutzern einen globalen Überblick über die Organisation. Jedoch sind nur bestimmte Geschäftsrollen berechtigt, die präsentierten Elemente zu erstellen oder zu ändern.

Um die Umgebung zu beschreiben, in der die Organisation tätig ist, können Sie in **MEGA** folgende Punkte definieren:

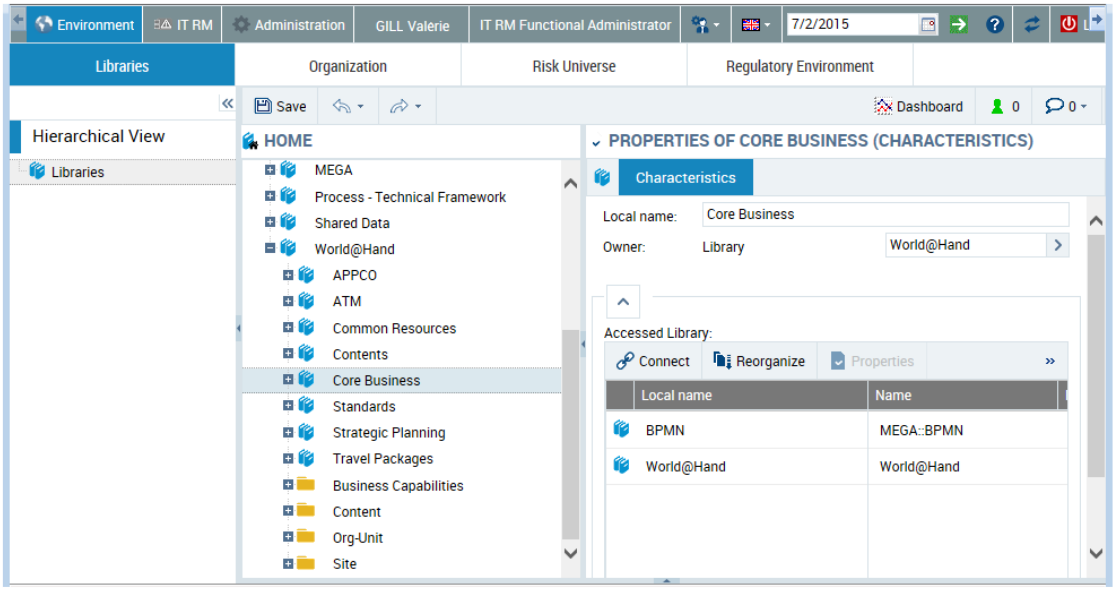
- ✓ "Die Bibliotheken", Seite 28
- ✓ "Die Organisation", Seite 29
- ✓ "Risiken und Kontrollen", Seite 36
- ✓ "Umgebung der Vorschriften", Seite 43
- ✓ "Finanzdaten", Seite 48
- ✓ "Ressourcen des Unternehmens", Seite 50
- ✓ "RACI", Seite 53

DIE BIBLIOTHEKEN

Bibliotheken sind Gruppierungen von Objekten, mit denen der Inhalt eines MEGA-Repositorys in mehrere unabhängige Teile unterteilt wird. Zwei Objekte aus verschiedenen Bibliotheken können somit denselben Namen tragen.

Um Bibliotheken zu verwalten, gehen Sie wie folgt vor:

- Wähle Sie den Desktop **Umgebung** aus und klicken Sie auf die Registerkarte **Bibliotheken**.



☛ *Weitere Informationen zu den Bibliotheken finden Sie im Handbuch **MEGA Common Features**, Kapitel "Bibliotheken".*

DIE ORGANISATION

Die Organisation eines Unternehmens ist in große Komponenten unterteilt:

- Prozesse

  Ein Geschäftsprozess stellt ein System dar, das Produkte oder Dienstleistungen an einen internen oder externen Kunden des Unternehmens oder Organisation liefert. Auf höherer Ebene definiert ein Geschäftsprozess eine Strukturierung und Kategorisierung des Geschäftsbereichs eines Unternehmens. Der Geschäftsprozess kann in weitere Prozesse unterteilt werden. Mit der Verbindung zu den organisatorischen Prozessen kann die reelle Implementierung des Geschäftsprozesses in der Organisation beschrieben werden. Ein Geschäftsprozess kann auch mit einer funktionalen Sicht detailliert werden.

  Ein organisatorischer Prozess beschreibt die Schritte, die durchgeführt werden müssen, um den Prozess zur Herstellung eines Produkts oder Flusses insgesamt oder teilweise umzusetzen.

- Entitäten

  Eine Entität kann eine unternehmensinterne oder -externe Entität sein: Eine interne Entität stellt ein Element der Organisation eines Unternehmens dar, wie beispielsweise eine Direktion, eine Abteilung oder einen Arbeitsplatz. Sie wird auf einer mehr oder weniger genauen Ebene definiert, je nachdem, wie präzise die Angaben über die Organisation sein müssen (siehe Organisationseinheitstyp). Beispiel: Finanzdirektion, Vertrieb, Marketingabteilung, Vertriebsmitarbeiter. Eine externe Organisationseinheit stellt eine Einrichtung dar, die Flüsse mit dem Unternehmen austauscht. Beispiel: Kunde, Lieferant, Administration.

- Geschäftssparten

  Eine Geschäftssparte ist eine Kompetenz oder eine Gruppierung von Kompetenzen im Interesse des Unternehmens. Sie entspricht zum Beispiel großen Produktsegmenten oder Distributionskanälen bzw. Geschäftstätigkeiten.

- Standorte

  Ein Standort ist der Ort, an dem sich das Unternehmen befindet. Standorte können Bezeichnungen von Standorttypen sein, z.B. Hauptsitz, Niederlassung, Fabrik, oder konkrete geografische Angaben, z.B. die Niederlassung in Berlin, die Fabrik in Bonn usw.

  ☛ *Die Standorte werden in **HOPEX IT Risk Management** nur informationshalber präsentiert. Sie werden in **MEGA IT Portfolio Management** verwendet.*

Diese Komponenten werden in Form einer Baumstruktur dargestellt.

Um auf diese Komponenten zuzugreifen, gehen Sie wie folgt vor:

1. Wählen Sie **Umgebung > Organisation > Hierarchische Ansichten** aus.
   In den Baumstrukturen können Sie zugreifen auf:
   - Prozesse
   - Entitäten
   - Geschäftssparten der Organisation

2. Wählen Sie in der betreffenden Baumstruktur ein Objekt aus.
   Das Eigenschaftsfenster des Objekts wird im rechten Teil der Lösung angezeigt.
3. Geben Sie die Eigenschaften ein oder verbinden Sie Kontextobjekte.

Die Prozesse

Um auf die Baumstruktur der Geschäftsprozesse zuzugreifen, gehen Sie wie folgt vor:

- Klicken Sie auf **Umgebung > Organisation Hierarchische Ansichten > Alle Prozesse**
  Wenn Sie den Ordner eines Prozesses aufklappen, kann die Baumstruktur der Unterprozesse eines aktuellen Prozesses angezeigt werden.

  ☛ *Die Liste der Prozesse im Besitz eines Prozesses kann in der Eigenschaftsseite des Prozesses, in der Registerkarte **Merkmale**, im Abschnitt **Unterprozess** geöffnet werden.*

Die Prozesstypen

Folgende Prozesstypen werden aufgeführt:

- Geschäftsprozess
- organisatorische Prozesse

Nach dem Typ wird beim Erstellen des Prozesses gefragt. Die beiden Typen werden mit einem Symbol in den Baumstrukturen und Listen voneinander unterschieden.

Geschäftsprozess

Mit einem Geschäftsprozess wird beschrieben, was ein Unternehmen "macht": sein Geschäftsbereich.

Der Prozess beantwortet die Frage "was?" Der Prozess beschreibt in erster Linie den Austausch der Informationsflüsse zwischen den verschiedenen Aktivitäten des Unternehmens.

Organisatorischer Prozess

Ein organisatorischer Prozess beschreibt die Schritte, die durchgeführt werden müssen, um den Prozess zur Herstellung eines Produkts oder Flusses insgesamt oder teilweise umzusetzen.

Die Merkmale eines Prozesses

Um auf die Merkmale eines Prozesses zuzugreifen, gehen Sie wie folgt vor:

- Klappen Sie im Eigenschaftsfenster des betroffenen Prozesses den Abschnitt **Merkmale** auf.

Für die Lenkung eines Prozesses sind Personen mit verschiedenen Funktionen verantwortlich.

- Der **Eigentümer** ist für den global funktionierenden Prozess in puncto Effizienz, Rentabilität und Sicherheit verantwortlich.
- Der **Durchführungsverantwortliche** trifft die Entscheidungen über den Ablauf des Prozesses und berichtet über den Fortschritt.
- Der **Ansprechpartner des Risikos** wird konsultiert, sobald eine Aktion im Zusammenhang mit Risiken geplant oder im Rahmen des Prozesses eingeleitet wird.

  ☛ *Das Feld **Ansprechpartner des Risikos** ist nur mit folgenden Lösungen verfügbar:*

  - ***HOPEX ERM***
  - ***HOPEX Internal Control***

Um die verantwortliche Person für die Lenkung eines Geschäftsprozesses anzugeben, gehen Sie wie folgt vor:

1. Klicken Sie im Eigenschaftsfenster eines Geschäftsprozesses auf die Registerkarte **Merkmale**.
2. Setzen Sie die Maus zum Beispiel auf das Feld **Eigentümer** und geben Sie die ersten Buchstaben des Namens ein.
3. Klicken Sie auf den Pfeil rechts neben dem Feld und wählen Sie **Personen auflisten** aus.
   Der Name der ausgewählten Person wird im Feld angegeben.

   🕮 *Eine Person wird mit ihrem Namen und ihrer E-Mail-Adresse definiert. Sie kann auf eine Anwendung zugreifen, sobald sie eine ID (Login) zur Verbindung erhalten hat. Auch eine oder mehrere Geschäftsrollen kann der Person zugewiesen werden.*
4. Im Anschluss klicken Sie auf **Speichern** oder wählen im Eigenschaftsfenster ein anderes Feld aus, um weitere Änderungen vorzunehmen.

Der Abschnitt Umfang eines Prozesses

Ein Prozess kann mit verschiedenen Komponententypen verbunden sein.

- **Entitäten**, die im Rahmen des Prozesses auftreten. Weitere Informationen finden Sie unter "Die Entitäten", Seite 32.
- **Geschäftssparten**, die die Services des Prozesses verwenden. Weitere Informationen finden Sie unter "Die Geschäftssparten der Organisation", Seite 34.
- **Risiken**, die bei Prozessen bestehen können. Weitere Informationen finden Sie unter "Die Risiken", Seite 36.
- **Kontrollen**, die bei Prozessen bestehen können. Weitere Informationen finden Sie unter "Die Kontrollen", Seite 40.
- **Vorfälle**
- **Aktionspläne**
- **Vorschriften**. Weitere Informationen finden Sie unter "Die Vorschriften", Seite 43.
- **Kontrollsysteme**

Die anderen Abschnitte eines Prozesses

Die Eigenschaftsseite eines Prozesses besteht aus folgenden Abschnitten:

- **RACI**: um die für den Prozess verantwortlichen Personen anzugeben. Weitere Informationen finden Sie unter "RACI", Seite 53.
- **Ziele und Anforderungen**: Weitere Informationen finden Sie unter "Ziele und Anforderungen", Seite 45.
- **Anlagen** : Weitere Informationen finden Sie im Handbuch **MEGA Common Features** im Kapitel "Geschäftsdokumente verwenden".
- **IT**: die Prozesse erhalten IT-Ressourcen für die notwendigen Vorgänge zur Umsetzung der Prozesse. Weitere Informationen finden Sie unter "Ressourcen des Unternehmens", Seite 50.

Die Entitäten

Eine Entität kann eine unternehmensinterne oder -externe Entität sein: Eine interne Entität stellt ein Element der Organisation eines Unternehmens dar, wie beispielsweise eine Direktion, eine Abteilung oder einen Arbeitsplatz. Sie wird auf einer mehr oder weniger genauen Ebene definiert, je nachdem, wie präzise die Angaben über die Organisation sein müssen (siehe Organisationseinheitstyp). Beispiel: Finanzdirektion, Vertrieb, Marketingabteilung, Vertriebsmitarbeiter. Eine externe Organisationseinheit stellt eine Einrichtung dar, die Flüsse mit dem Unternehmen austauscht. Beispiel: Kunde, Lieferant, Administration.

Zugriff auf die Entitäten der Organisation

Um die Liste der betroffenen Entitäten der Organisation zu definieren, können Sie in **MEGA** das Organigramm des Unternehmens eingeben.

Um auf die Entitäten der Organisation zuzugreifen, gehen Sie wie folgt vor:

1. Klicken Sie auf **Umgebung > Organisation > Hierarchische Ansichten > Entitäten**
2. Klappen Sie die Stammentität auf.
   Daraufhin wird die Liste der Entitäten dieser Organisation angezeigt.

   ☛ *Die Liste der Entitäten im Besitz einer Entität kann in der Eigenschaftsseite der Entität, in der Registerkarte **Merkmale**, im Abschnitt **Unterentitäten** geöffnet werden.*

Entität erstellen

Um eine neue Entität zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie auf **Umgebung > Organisation > Hierarchische Ansichten > Entitäten**
2. Öffnen Sie die Eigenschaftsseite der Entität, die im Besitz der zu erstellenden Entität ist.
3. Klicken Sie im Abschnitt **Unterentitäten** auf die Schaltfläche **Neu**. Daraufhin wird das Fenster zum Erstellen einer Entität geöffnet.
4. Geben Sie den **Namen** der Entität ein und klicken Sie auf **OK**. Die neue Entität wird in der Liste aufgeführt.
5. Öffnen Sie die Eigenschaftsseite der erstellten Entität.
6. Ändern Sie eventuell die **Übergeordnete Entität**, die der Ebene entspricht, auf der Sie in der Baumstruktur positioniert sind, um die Entität zu erstellen.

   ☛ *Das Feld **Übergeordnete Entität** wird automatisch und abhängig von der Position der Entität in der Baumstruktur errechnet.*
7. Geben Sie die **Ebene** der Entität in der Organisation an:
   - "Division"
   - "Abteilung"
   - "Sektion"
8. Geben Sie den **Status**, "Aktiv" oder "Inaktiv "der Entität an.
9. Im Anschluss klicken Sie auf **Speichern** oder wählen im Eigenschaftsfenster ein anderes Feld aus, um weitere Änderungen vorzunehmen.

Ansprechpartner des Risikos

Um die verantwortliche Person der Risikobewertung bei der Entität anzugeben, gehen Sie wie folg vor:

1. Wählen Sie im Feld **Ansprechpartner des Risikos** die betroffene Person aus.

   ☛ *Sie müssen dieses Feld im Rahmen einer Risikobewertung durch Kampagnen mit **HOPEX ERM** unbedingt ausfüllen.*

   ☛ *Das Feld Ansprechpartner ist nur mit folgenden Lösungen verfügbar:*
   - ***HOPEX ERM***
   - ***HOPEX Internal Control***

Der Abschnitt Umfang

Eine Entität kann im Rahmen eines Prozesses verwendet werden. Sie kann hierarchisch unterteilt werden:

Eine Entität kann mit verschiedenen Komponententypen verbunden sein.

- **Entitäten**: Sie können die verantwortliche Entität einer Sektion oder einer Direktion sowie die funktionale Abhängigkeit zwischen den beiden Entitäten angeben.
- **Geschäftsprozesse** und **organisatorische Prozesse** , für die die Entität eintritt. Weitere Informationen finden Sie unter "Die Prozesse", Seite 30.
- **Risiken**, das Management wird von der Entität übernommen. Weitere Informationen finden Sie unter "Die Risiken", Seite 36.
- **Kontrollen**, das Management wird von der Entität übernommen. Weitere Informationen finden Sie unter "Die Kontrollen", Seite 40.
- **Ziele** und **Anforderungen**, die der Entität zugewiesen wurden. Weitere Informationen finden Sie unter "Ziele und Anforderungen", Seite 45.

  ☛ *Einige wichtige Dokumente, wie zum Beispiel strategische Pläne, der Business Pan, Jahresberichte, Wirtschaftsanalysen und andere relevante Dokumente für die Organisation und ihre Ziele können für die Festlegung der **Ziele** und **Anforderungen** aufgerufen werden.*
- **Geschäftssparten**, bei denen die Entität verwendet wird. Weitere Informationen finden Sie unter "Die Geschäftssparten der Organisation", Seite 34.

  ☛ *Je nach Ihren Rechten können Sie auch die **Aktionspläne** oder Vorfälle anzeigen, bei denen die Entität der Eigentümer ist.*

Die Geschäftssparten der Organisation

In der Gesamtansicht der Geschäftssparten werden die verschiedenen Geschäftsbereiche des Unternehmens präsentiert.

🕮 *Eine Geschäftssparte ist eine Kompetenz oder eine Gruppierung von Kompetenzen im Interesse des Unternehmens. Sie entspricht zum Beispiel großen Produktsegmenten oder Distributionskanälen bzw. Geschäftstätigkeiten.*

Zugriff auf die Geschäftssparten

Um auf die Geschäftssparten der Organisation zuzugreifen, gehen Sie wie folgt vor:

❱ Wählen Sie **Umgebung > Organisation > Hierarchische Ansichten > Geschäftssparten** aus.
Auf dieser Seite können Sie in Form einer Baumstruktur die Geschäftssparten der Organisation anzeigen, ihre Eigenschaften aufrufen und neue Objekte erstellen.

☛ *Die Liste der Geschäftssparten im Besitz der Geschäftssparte kann auf der Eigenschaftsseite einer Geschäftssparte im Abschnitt **Geschäftsuntersparten** geöffnet werden.*

Um auf die Merkmale einer Geschäftssparte zuzugreifen, gehen Sie wie folgt vor:

❱ Klappen Sie im Eigenschaftsfenster der betroffenen Geschäftssparte den Abschnitt **Merkmale** auf.

Umfang der Geschäftssparten

Eine Geschäftssparte kann implementiert werden von:

- **OrgEinheiten**. Ausführliche Informationen finden Sie unter "Die Entitäten", Seite 32.
- **Anwendungen**. Ausführliche Informationen finden Sie unter "Die Anwendungen", Seite 50.

  ☛ *Die Anwendungen sind in der Lösung **HOPEX Regulatory Compliance** nicht verfügbar.*
- **Risiken**

Eine Geschäftssparte kann mit verschiedenen Komponententypen verbunden werden, beispielsweise **Geschäftsbereiche** und **organisatorische Prozesse**, die die Services der Geschäftssparte verwenden. Weitere Informationen finden Sie unter "Die Prozesse", Seite 30.

☛ *In **HOPEX IT Risk Management** ist der Abschnitt **Umfang** nur informationshalber enthalten.*

RISIKEN UND KONTROLLEN

Um auf die Risiken der Organisation zuzugreifen, gehen Sie wie folgt vor:

❱ Klicken Sie im Desktop **Umgebung** auf **Risikouniversum**.

☛ *In den **MEGA**-Lösungen haben Sie ab der Registerkarte **Bibliothek** ebenfalls Zugriff auf die Risiken.*

Die Risiken

Zugriff auf die Risiken

Um auf die Risiken zuzugreifen, gehen Sie wie folgt vor:

❱ Klicken Sie auf **Umgebung >Risikouniversum > Risiken > Alle Risiken** .

☛ *Sie können auch im Abschnitt **Umfang** der Seite des Kontrollsystems die Risiken anzeigen, die von einem Kontrollsystem abgedeckt werden. Weitere Informationen finden Sie unter "Die Kontrollen", Seite 40.*

Um auf die wichtigsten Risiken zuzugreifen, gehen Sie wie folgt vor:

❱ Klicken Sie auf **Umgebung >Risikouniversum > Risiken > Hauptrisiken** .

Merkmale eines Risikos

Um auf die Merkmale eines Risikos zuzugreifen, gehen Sie wie folgt vor:

❱ Wählen Sie in einer Liste der Risiken oder Hauptrisiken ein Risiko aus und klicken Sie auf die Schaltfläche **Eigenschaften**.
Die Eigenschaftsseite des Risikos wird im rechten Fenster angezeigt.

Auf dieser Seite können Sie folgende Informationen angeben:

- den **Identifizierungscode** des Risikos
- den **Namen** des Risikos
- dass das Risiko erhöht ist, wenn Sie eventuell das Kästchen **Hauptrisiko** markieren
- den **Eigentümer** des Risikos
- den **Identifizierungsmodus** des Risikos
  Das Risiko kann beispielsweise identifiziert werden durch:
  - ein "Ereignis-Repository"
  - einen "Workshop"
  - eine "Stichprobe"
  - einen "Audit-Auftrag"
- die **detaillierte Beschreibung** des Risikos

☛ *Der **Status des Risikos** kann nicht geändert werden, da er vom Workflow des Risikos verwaltet wird. Ausführliche Informationen finden Sie unter **HOPEX ERM**.*

Der Umfang eines Risikos

Im Umfang des Risikos kann die Lokalisierung eines Risikos definiert werden. Im Umfang sind mehrere Komponententypen enthalten:

- **Entitäten**, die vom Risiko betroffen sind. Weitere Informationen finden Sie unter "Die Entitäten", Seite 32.

  Eine Entität kann eine unternehmensinterne oder -externe Entität sein: Eine interne Entität stellt ein Element der Organisation eines Unternehmens dar, wie beispielsweise eine Direktion, eine Abteilung oder einen Arbeitsplatz. Sie wird auf einer mehr oder weniger genauen Ebene definiert, je nachdem, wie präzise die Angaben über die Organisation sein müssen (siehe Organisationseinheitstyp). Beispiel: Finanzdirektion, Vertrieb, Marketingabteilung, Vertriebsmitarbeiter. Eine externe Organisationseinheit stellt eine Einrichtung dar, die Flüsse mit dem Unternehmen austauscht. Beispiel: Kunde, Lieferant, Administration.

- **Geschäftsprozesse** und **organisatorische Prozesse**, die dem Risiko ausgesetzt sind. Weitere Informationen finden Sie unter "Die Prozesse", Seite 30.

  Ein Geschäftsprozess stellt ein System dar, das Produkte oder Dienstleistungen an einen internen oder externen Kunden des Unternehmens oder Organisation liefert. Auf höherer Ebene definiert ein Geschäftsprozess eine Strukturierung und Kategorisierung des Geschäftsbereichs eines Unternehmens. Der Geschäftsprozess kann in weitere Prozesse unterteilt werden. Mit der Verbindung zu den organisatorischen Prozessen kann die reelle Implementierung des Geschäftsprozesses in der Organisation beschrieben werden. Ein Geschäftsprozess kann auch mit einer funktionalen Sicht detailliert werden.

  Ein organisatorischer Prozess beschreibt die Schritte, die durchgeführt werden müssen, um den Prozess zur Herstellung eines Produkts oder Flusses insgesamt oder teilweise umzusetzen.

- **Ziele und Anforderungen** , die gegenüber dem Risikomanagement erwartet werden. Weitere Informationen finden Sie unter "Ziele und Anforderungen", Seite 45.

  Ein Ziel ist ein Ergebnis, das erreicht werden soll, oder das angestrebte Resultat eines Prozesses oder eines Arbeitsschritts. Mit einem Ziel können die Punkte hervorgehoben werden, die für diesen Prozess oder diesen Arbeitsschritt verbessert werden sollen.

  Eine Anforderung ist ein explizit ausgedrückter Bedarf oder eine Erwartung, die wie eine Einschränkung vorgeschrieben und im Rahmen eines Zertifikations-, Organisations- oder Modifikationsprojekts für das Informationssystem des Unternehmens erfüllt werden muss.

- **Anwendungen**. Ausführliche Informationen finden Sie unter "Die Anwendungen", Seite 50.

  Eine Anwendung besteht aus Software-Komponenten, die im Rahmen der IT-Entwicklungen eine konsistente Einheit bilden.

- **Geschäftssparten**. Ausführliche Informationen finden Sie unter "Die Geschäftssparten der Organisation", Seite 34.

  Eine Geschäftssparte ist eine Kompetenz oder eine Gruppierung von Kompetenzen im Interesse des Unternehmens. Sie entspricht zum Beispiel großen Produktsegmenten oder Distributionskanälen bzw. Geschäftstätigkeiten.

Analyse eines Risikos

Mit einer Risikoanalyse soll das Risiko gut verstanden werden.

Die Risikoanalyse muss Folgendes berücksichtigen:

- die Risikoursachen
- die positiven und negativen Folgen bzw. Konsequenzen dieses Risikos

In der Analysephase kann ein Risiko verbunden werden mit:

- Risikotypen
- Risikofaktoren
- Folgen
- anderen Risiken

Um ein Risiko zu analysieren, gehen Sie wie folgt vor:

1. Wählen Sie ein Risiko aus und öffnen Sie die Eigenschaftsseite des Risikos.
2. Klappen Sie unter der Registerkarte **Merkmale** den Abschnitt **Analyse** auf.
   Ein Risiko zeichnet sich wie folgt aus:
   - durch **Risikotypen**. Weitere Informationen finden Sie unter "Die Risikotypen", Seite 38.

     Ein Risikotyp definiert die Typologie eines normalisierten Risikos im Rahmen einer Organisation.
   - durch **Risikofaktoren**. Weitere Informationen finden Sie unter "Risikofaktoren", Seite 39.

     Ein Risikofaktor ist ein Element, das zum Auftreten eines Risikos beiträgt oder ein Risiko auslöst. Für verschiedene Risiken kann ein und derselbe Risikofaktor verantwortlich sein. Beispiele: Die Verwendung eines gefährlichen chemischen Produkts, eine komplexe Anwendung, die Größe eines Projekts, die Anzahl der Mitwirkenden, eine neue Technik, mangelnde Qualitätssicherung, mangelnde Sorgfalt bei der Festlegung der Anforderungen usw.
   - durch **Risikofolgen**. Weitere Informationen finden Sie unter "Risikofolgen", Seite 39.

     Die Folge eines Risikos kann positiv oder negativ sein. Sie wird mit einem Typ verbunden, mit dem sich die Folge charakterisieren lässt. Beispiel: Bild, Umgebung, Angestellte.
   - **Verbundene Risiken**
   - **Vorfälle**

     Ein Vorfall ist ein Fakt einer internen oder externen Quelle, der sich auf die Organisation auswirkt. Er bildet das Grundelement für die Sammlung von Daten über ein Betriebsrisiko.

Die Risikotypen

Ein Risikotyp definiert die Typologie eines normalisierten Risikos im Rahmen einer Organisation.

Ein Risikotyp charakterisiert ein Risiko. Ein Risiko kann zum Beispiel den Typ vorschriftsmäßig, rechtlich, technisch, usw. haben.

Die Zusammensetzung des Risikotyps hängt von den verschiedenen Aktivitäten und des Geschäftsbereichs ab. Die allgemeinen Risikotypen können sich mehr oder weniger aus spezifischen Risikotypen zusammensetzen.

Es ist wichtig, einen Risikotyp so zu definieren, dass er sich identifizieren, messen und verwalten lässt. Ebenso muss die Anzahl der verschiedenen Risikostufen begrenzt werden, um eine nützliche Nomenklatur zu erhalten.

Mit der Freigabe der Nomenklatur muss sichergestellt werden, dass ein Risikotyp, der in zwei verschiedenen Entitäten oder Aktivitäten definiert wurde, dieselbe Definition und dieselbe Bedeutung hat, um ein kohärentes System zu erhalten.

Da dieses System ebenfalls den Vorschriften genügen muss, muss eine zweite Nomenklatur definiert werden, um die deklarativen Aspekte zu berücksichtigen und um dem Informationsaustausch mit den Kontrollsystemen zu genügen.

Um eigene Risikotypen zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie das Navigationsfenster **Umgebung > Risikouniversum > Risiken > Risikotypen** aus.
2. Klicken Sie im Kontextmenü des Ordners "Risikotyp" auf den Befehl **Neu**.
3. Geben Sie den Namen des Risikotyps ein und klicken Sie auf **OK**.
   In der Baumstruktur des Navigators wird der neue Risikotyp angezeigt.

   ☛ *Auf gleiche Weise können Sie ab einem Risikotyp einen Risikountertyp erstellen.*

Risikofaktoren

Viele Risikofaktoren werden im Rahmen internationaler, nationaler Bestimmungen, Vorschriften innerhalb verschiedener Berufsverbände oder im Unternehmen selbst definiert.

🕮 *Ein Risikofaktor ist ein Element, das zum Auftreten eines Risikos beiträgt oder ein Risiko auslöst. Für verschiedene Risiken kann ein und derselbe Risikofaktor verantwortlich sein. Beispiele: Die Verwendung eines gefährlichen chemischen Produkts, eine komplexe Anwendung, die Größe eines Projekts, die Anzahl der Mitwirkenden, eine neue Technik, mangelnde Qualitätssicherung, mangelnde Sorgfalt bei der Festlegung der Anforderungen usw.*

Jedem Risiko können ein oder mehrere Risikofaktoren zugeordnet werden, die Risikoquellen oder Gefahren darstellen, die den Betrieb der Organisation potenziell gefährden können. Beispiel: gefährliche chemische Produkte, Konkurrenten, Regierungen usw.

Risikofolgen

Um die Folgen eines Risikos zu definieren, gehen Sie wie folgt vor:

- Klicken Sie auf der Seite eines Risikos, im Abschnitt **Analyse**, Registerkarte **Risikofolgen** auf die Registerkarte **Neu**.
  Daraufhin wird die Seite zum Erstellen einer Folge geöffnet.

  ☛ *Eine Risikofolge kann sich nur auf ein einziges Risiko beziehen. Daher ist das aktuelle Risiko im Feld **Risiko** bereits angegeben.*

Im Abschnitt **Risikofolgen** können Sie den **Identifizierungscode** der Folge angeben.

Die erstellte Folge wird in der Liste der Folgen des betreffenden Risikos aufgeführt.

RACI bei einem Risiko

Auf der Eigenschaftsseite eines Risikos wird der Abschnitt **RACI** aufgeführt, um die im Risikomanagement eingebundenen verschiedenen verantwortlichen Personen festzulegen. Weitere Informationen finden Sie unter "RACI", Seite 53.

Die Kontrollen

Um auf die Kontrollen zuzugreifen, gehen Sie wie folgt vor:

❱ Klicken Sie im Desktop **Umgebung** auf **Risikouniversum > Kontrollen**.

Merkmale einer Kontrolle

Um auf die Merkmale einer Kontrolle zuzugreifen, gehen Sie wie folgt vor:

❱ Wählen Sie die betreffende Kontrolle in der Liste aus und klicken Sie auf die Schaltfläche **Eigenschaften**.
Die Eigenschaftsseite wird im rechten Fenster angezeigt.

Auf dieser Seite können Sie folgende Informationen angeben:

- den **Code** zur eindeutigen Identifizierung der Kontrolle.
- den **Namen** der Kontrolle.
- das **Ziel** der Kontrolle.
- den **Eigentümer** der Kontrolle.
- inwieweit die Kontrolle wichtig ist, wenn Sie das Kontrollkästchen **Hauptkontrolle** markieren
- die **Art** der Kontrolle. Sie haben folgende Auswahl:
  - "Berichtigung"
  - "Ermittlung"
  - "Prävention"
- die **Operativen Kosten** für die Implementierung der Kontrolle.
- den **Ausführungsmodus**, mit dem angegeben wird, wie die Kontrolle ausgeführt wird:
  - "Automatisch": Die Kontrolle wird vollkommen automatisch von einer IT-Anwendung durchgeführt.
  - "Manuell": Die Kontrolle wird manuell von einer Entität der Organisation durchgeführt.
  - "Halbautomatisch": Die Kontrolle wird von einer Entität der Organisation durchgeführt, die von einer IT-Anwendung unterstützt wird.
- den **Status**
  - "Entwurf"
  - "Freigegeben"

☛ *Sie können dieses Feld manuell zur Information ausfüllen.*

☛ *Die Felder können von der jeweils verwendeten Lösung abhängen.*

RACI bei einer Kontrolle

Auf der Eigenschaftsseite einer Kontrolle wird der Abschnitt **RACI** aufgeführt, um die im Management dieser Kontrolle verschiedenen eingebundenen verantwortlichen Personen festzulegen. Weitere Informationen finden Sie unter "RACI", Seite 53.

Der Umfang einer Kontrolle

Im Umfang der Kontrolle kann die Lokalisierung einer Kontrolle definiert werden. Im Umfang sind mehrere Komponententypen enthalten:

- **Geschäftsprozesse** und **organisatorische Prozesse**, die dem Risiko ausgesetzt sind, die von der Kontrolle abgedeckt werden. Weitere Informationen finden Sie unter "Die Prozesse", Seite 30.
- **Entitäten**, die von den Kontrollen betroffen sind. Weitere Informationen finden Sie unter "Die Entitäten", Seite 32.
- **Risiken**, die von den Kontrollen abgedeckt sind. Weitere Informationen finden Sie unter "Die Risiken", Seite 36.
- **Anforderungen**, die gegenüber dem Risikomanagement erwartet werden. Weitere Informationen finden Sie unter "Ziele und Anforderungen", Seite 45.
- die **Kontrolltypen** Weitere Informationen finden Sie unter "Die Kontrolltypen", Seite 41.
- die **Arbeitsschritte**

  Ein Arbeitsschritt ist eine elementare Etappe eines organisatorischen Prozesses und entspricht dem Einschreiten einer Organisationseinheit entspricht.
- die **Konten**: siehe "Die Finanzkonten", Seite 49.
- die **Vorfälle**: je nach Lösung können Sie die Vorfälle anzeigen (ohne sie ändern zu können).

  Ein Vorfall ist ein Fakt einer internen oder externen Quelle, der sich auf die Organisation auswirkt. Er bildet das Grundelement für die Sammlung von Daten über ein Betriebsrisiko.

Die Kontrolltypen

Mit dem oder den Kontrolltypen werden die Vorschriften angegeben, die für eine Kontrolle gelten.

Diese Kontrollen können definiert werden, indem die Kontrolltypen berücksichtigt werden, die im Rahmen des betroffenen Kontroll- und Risikosystems festgelegt wurden.

```
Eine der oft verwendeten Kontrollnomenklaturen ist die
Nomenklatur, die von der COBIT definiert wurde.

COBIT bedeutet "Control Objectives for Information and
Related Technology".

COBIT ist ein Rahmenwerk der Best Practices (besten
Vorgehensweisen), in das viele weitere Rahmenwerke
eingebunden sind und das von vielen internationalen
Experten unterstützt wird. Den 34 von COBIT definierten
Prozessen entsprechen 318 Kontrollziele, für die
```

detaillierte Kontrollpraktiken identifiziert wurden. Der Leitfaden zur Überprüfung beschreibt die erforderlichen Elemente, um jeden Prozess richtig verstehen zu können, führt die durchzuführenden Kontrollen auf, liefert die Elemente für die Beurteilung der Einhaltung der Best Practices und für die Beurteilung der Risiken, die festgelegten Ziele nicht zu erreichen.

Um auf die Kontrolltypen zuzugreifen, gehen Sie wie folgt vor:

- Klicken Sie auf **Umgebung> Risikouniversum > Kontrollen > Kontrolltypen**"
  Es wird eine Liste der Kontrolltypen angezeigt.

  Mit einem Kontrolltyp lassen sich die Kontrollen klassieren, die im Unternehmen entsprechend des Standards bzw. Normen der betreffenden Sektoren oder Vorschriften/Reglementierungen (Cobit usw.) implementiert sind.

UMGEBUNG DER VORSCHRIFTEN

Die Umgebung der Vorschriften eines Unternehmens kann aus folgenden Elementen bestehen:

- Vorschriften
- Ziel
- Anforderungen

Um auf diese Komponenten zuzugreifen, gehen Sie wie folgt vor:

1. Klicken Sie im Desktop Umgebung auf **Umgebung der Vorschriften> Vorschriften**.

Die Vorschriften

Mögliche zu berücksichtigende Vorschriften:

- Finanzen (SOX, LSF)
- Sektoren (Basel II, Solvency II, Seveso II)
- im Zusammenhang mit Personenschutz zum Beispiel.

> *Eine Vorschrift oder eine interne Regelung stellt mehrere Richtlinien mit oder ohne Bedingungen auf, die von der Regierung im Rahmen eines Gesetzes, von einem Berufsverband in Form von Best Practices oder intern von einer Organisation festgelegt werden.*
>
> *Auch organisationsinterne Vorschriften können als Governance-Leitfaden dienen.*
>
> *In dieser Dokumentation wird der Begriff "Vorschriften" verwendet, unabhängig davon ob sie organisationsextern oder -intern sind.*

Zugriff auf die Vorschriften der Organisation

Für den Zugriff auf die Liste der Vorschriften gehen Sie wie folgt vor:

1. Wählen Sie **Umgebung > Umgebung der Vorschriften > Vorschriften** aus.
   Daraufhin wird die Liste der Vorschriften dieser Umgebung angezeigt.

Merkmale einer Vorschrift

Um auf die allgemeinen Merkmale einer Vorschrift zuzugreifen, gehen Sie wie folgt vor:

1. Wählen Sie auf der Seite mit den Vorschriften die gewünschte Vorschrift aus und klicken Sie auf **Eigenschaften**.
   Sie können die Merkmale der Vorschrift aufrufen oder ändern:
   - den **Vorschriftencode**
   - Das **Anfangsdatum**, ab dem die Vorschrift gilt
   - Das **Enddatum**, bis zu dem die Vorschrift gilt

Sie können ebenfalls:

- Elemente von RACI angeben: siehe "RACI", Seite 53.
- den Umfang er Vorschrift definieren:
  - Anforderungen

    📖 *Eine Anforderung ist ein explizit ausgedrückter Bedarf oder eine Erwartung, die wie eine Einschränkung vorgeschrieben und im Rahmen eines Zertifikations-, Organisations- oder Modifikationsprojekts für das Informationssystem des Unternehmens erfüllt werden muss.*
  - Risikotypen

    📖 *Ein Risikotyp definiert die Typologie eines normalisierten Risikos im Rahmen einer Organisation.*
  - Risikofaktoren

    📖 *Ein Risikofaktor ist ein Element, das zum Auftreten eines Risikos beiträgt oder ein Risiko auslöst. Für verschiedene Risiken kann ein und derselbe Risikofaktor verantwortlich sein. Beispiele: Die Verwendung eines gefährlichen chemischen Produkts, eine komplexe Anwendung, die Größe eines Projekts, die Anzahl der Mitwirkenden, eine neue Technik, mangelnde Qualitätssicherung, mangelnde Sorgfalt bei der Festlegung der Anforderungen usw.*
  - Risikofolgen

    📖 *Die Folge eines Risikos kann positiv oder negativ sein. Sie wird mit einem Typ verbunden, mit dem sich die Folge charakterisieren lässt. Beispiel: Bild, Umgebung, Angestellte.*
  - Kontrollsysteme

    📖 *Ein Kontrollsystem besteht aus mehreren Kontrollen, mit denen Risiken für ein Unternehmen verhütet und Risiken unter Kontrolle gehalten werden können, sowie interne Betriebsregeln angewendet, Gesetze oder Vorschriften eingehalten oder strategische Ziele des Unternehmens erreicht werden können.*
  - Geschäftssparten

    📖 *Eine Geschäftssparte ist eine Kompetenz oder eine Gruppierung von Kompetenzen im Interesse des Unternehmens. Sie entspricht zum Beispiel großen Produktsegmenten oder Distributionskanälen bzw. Geschäftstätigkeiten.*
  - Geschäftsprozesse und organisatorische Prozesse

    📖 *Ein Geschäftsprozess stellt ein System dar, das Produkte oder Dienstleistungen an einen internen oder externen Kunden des Unternehmens oder Organisation liefert. Auf höherer Ebene definiert ein Geschäftsprozess eine Strukturierung und Kategorisierung des Geschäftsbereichs eines Unternehmens. Der Geschäftsprozess kann in weitere Prozesse unterteilt werden. Mit der Verbindung zu den organisatorischen Prozessen kann die reelle Implementierung des Geschäftsprozesses in der Organisation beschrieben werden. Ein Geschäftsprozess kann auch mit einer funktionalen Sicht detailliert werden.*

    📖 *Ein organisatorischer Prozess beschreibt die Schritte, die durchgeführt werden müssen, um den Prozess zur Herstellung eines Produkts oder Flusses insgesamt oder teilweise umzusetzen.*
  - Untervorschriften: im Rahmen von **HOPEX IT Risk Management**.

Ziele und Anforderungen

Um sicherzustellen, dass Ihre Organisation die strategischen Erwartungen des Unternehmens erfüllen, können die wichtigsten **MEGA** -Konzepte mit Zielen und Anforderungen verbunden werden.

> 🕮 *Eine Anforderung ist ein explizit ausgedrückter Bedarf oder eine Erwartung, die wie eine Einschränkung vorgeschrieben und im Rahmen eines Zertifikations-, Organisations- oder Modifikationsprojekts für das Informationssystem des Unternehmens erfüllt werden muss.*

Als Erstes sollten die Ziele erfasst werden, sowie die vorgeschriebenen Anforderungen, um sie mit den wichtigsten organisatorischen und technischen Komponenten zu verbinden.

> 🕮 *Ein Ziel ist ein Ergebnis, das erreicht werden soll, oder das angestrebte Resultat eines Prozesses oder eines Arbeitsschritts. Mit einem Ziel können die Punkte hervorgehoben werden, die für diesen Prozess oder diesen Arbeitsschritt verbessert werden sollen.*

Auf Ziele und Anforderungen zugreifen

Um auf die Baumstruktur der Ziele zuzugreifen, gehen Sie wie folgt vor:

- Klicken Sie auf **Umgebung > Umgebung der Vorschriften > Ziele**.
  Daraufhin werden die Ziele der Organisation hierarchisch angezeigt.
  Wenn Sie den Ordner eines Ziels aufklappen, kann die Baumstruktur der Unterziele eines aktuellen Ziels angezeigt werden.

  > ☛ *Die Liste der Ziele im Besitz eines Ziels kann in der Eigenschaftsseite des Ziels, in der Registerkarte **Merkmale**, im Abschnitt **Unterziele** geöffnet werden.*

Um auf die Baumstruktur der Anforderungen zuzugreifen, gehen Sie wie folgt vor:

- Wählen Sie **Umgebung > Umgebung der Vorschriften > Anforderungen** aus.
  Daraufhin werden die Anforderungen der Organisation hierarchisch angezeigt.
  Wenn Sie den Ordner einer Anforderung aufklappen, kann die Baumstruktur der Unteranforderungen der aktuellen Anforderungen angezeigt werden.

  > ☛ *Die Liste der Anforderungen im Besitz einer Anforderung kann in der Eigenschaftsseite der Anforderung, in der Registerkarte **Merkmale**, im Abschnitt **Unteranforderungen** geöffnet werden.*

Merkmale der Ziele

Ein Ziel kann quantitativ, das heißt direkt messbar, oder qualitativ sein.

- Die Frist zwischen Bestellung und Lieferung verkürzen (quantitatives Ziel)
- Die Qualität des Produkts verbessern (qualitatives Ziel)
- Die Kundenzufriedenheit erhöhen (qualitatives Ziel)

Sie können ein Ziel mit verschiedenen Komponententypen verbinden.

- **Entitäten**: Ausführliche Informationen finden Sie unter "Die Entitäten", Seite 32.
- **Geschäftsprozesse** und **organisatorische Prozesse**: Ausführliche Informationen finden Sie unter "Die Prozesse", Seite 30.
- **Risiken**: Ausführliche Informationen finden Sie unter "Die Risiken", Seite 36.
- **Kontrollen**: Ausführliche Informationen finden Sie unter "Die Kontrollen", Seite 40.
- **Geschäftssparten**: Ausführliche Informationen finden Sie unter "Die Geschäftssparten der Organisation", Seite 34.

Merkmale der Anforderungen

Um auf die Eigenschaften einer Anforderung zuzugreifen, gehen Sie wie folgt vor:

1. Wählen Sie auf der Seite mit den Anforderungen die gewünschte Anforderung aus und klicken Sie auf **Eigenschaften**.
   Sie können die Merkmale der Anforderung aufrufen oder ändern:

   ☛ *Laut der Norm ISO 9000, "ist eine Anforderung ein(e) explizit ausgedrückte(r) Bedarf oder Erwartung, die in der Regel implizit ist oder auferlegt wurde. Die Norm ISO 9000 legt den Schwerpunkt auf die "Kundenerwartungen", aber im Rahmen eines Projekts sind weitere Anforderungen in Betracht zu ziehen (beispielsweise die Auflagen der Direktion, die Einhaltung von Empfehlungen, usw.)*

Die Priorität kann verschiedene Stufen haben:

- Schwach
- Durchschnitt
- Stark

Umfang einer Anforderung

Sie können eine Anforderung mit verschiedenen Objekttypen verbinden.

☛ *Es hängt von der verwendeten Lösung ab, welche Objekttypen verbunden werden können.*

Um auf die Objekte des Umfangs einer Anforderung zuzugreifen, gehen Sie wie folgt vor:

1. Klicken Sie im Eigenschaftsfenster der Anforderung auf die Registerkarte **Umfang**.
   Die Geschäftsprozesse und organisatorischen Prozesse, die Entitäten und Anwendungen werden in der Registerkarte **Umfang** unter den beiden Abschnitten abhängig von der Rolle angezeigt:
   - **Eingeschränktes Element**: Objekte, die die Anforderung erfüllen müssen

     ```
     Der Prozess "Abwicklung der Ausschreibungen" muss die
     Anforderung "Segregation of duties" erfüllen.
     ```
   - **Beitragendes Element**: Objekte, die zur Erfüllung der Anforderung beitragen.

     ```
     Die Anwendung "Ausschreibung" kann eine Kontrolle
     automatisieren, um zu überprüfen, ob der Prozess die
     Anforderungen erfüllt.
     ```
   - **Vorfälle**: Vorfälle, bei denen die Anforderung nicht erfüllt wurde.
   - **Unteranforderungen**

     ☛ *In **HOPEX IT Risk Management** werden keine Unteranforderungen verwendet.*

Risiken und Kontrollen

Um auf die Risiken und Kontrollen zuzugreifen, die mit einer Anforderung verbunden sind, gehen Sie wie folgt vor:

1. Klappen Sie im Eigenschaftsfenster der Anforderung den Abschnitt **Risiken und Kontrollen** auf.

   ☛ *Weitere Informationen finden Sie unter "Die Risiken", Seite 36 und "Die Kontrollen", Seite 40.*

FINANZDATEN

Um auf die Produkte und Konten der Organisation zuzugreifen, gehen Sie wie folgt vor:

❱ Klicken Sie im Desktop **Umgebung** auf **Finanzdaten**.

✓ "Die Produkte", Seite 48
✓ "Die Finanzkonten", Seite 49

☛ *Diese Navigationsregisterkarte ist in der Lösung **HOPEX IT Risk Management** nicht verfügbar.*

Die Produkte

Eine Geschäftssparte ist mit Produkten verbunden, die ein Unternehmen auf dem Markt anbietet. Diese Produkte bilden eine Verbindung zwischen der Geschäftssparte und den Prozessen, die für die Produktion sorgen.

📖 *Ein Produkt stellt einen oder mehrere Artikel, Objekte, Produkte oder Dienstleistungen als Ergebnis einer Aktivität in der Landwirtschaft, der Industrie oder des Dienstleistungsbereichs dar, die von einem Unternehmen angeboten werden.*

☛ *Ein Produkt kann auf seiner Eigenschaftsseite in Unterprodukte unterteilt werden.*

Um ab einem existierenden Produkt ein neues Produkt zu erstellen, gehen Sie wie folgt vor:

1. Zeigen Sie die Baumstruktur der Produkte an
2. Klicken Sie auf das betreffende Produkt.
   Die Eigenschaftsseite wird im rechten Teil des Bildschirms geöffnet.
3. Klicken Sie im Abschnitt **Unterprodukt** auf die Schaltfläche **Neu**.
   Das neue Produkt wird in der Liste der Produkte angezeigt, die das beschriebene Produkt bilden.
4. Wählen Sie das soeben erstellte Produkt aus, drücken Sie auf die Taste <F2> und ändern Sie den Produktnamen.

Um den Produkttyp anzugeben, gehen Sie wie folgt vor:

1. Öffnen Sie das Eigenschaftsfenster des betreffenden Produkts.
2. Wählen Sie im Feld **Produkttyp** den einen Wert:
   - Produkte
   - Komplex
   - Dienste

In einem Abschnitt können Sie zudem die Vorfälle erstellen und anzeigen, die bei diesem Produkt eingetreten sind.

☛ *Dieser Objekttyp ist in der Lösung **HOPEX IT Risk Management** nicht verfügbar.*

Die Finanzkonten

MEGA ermöglicht, Konten einer Entität zu definieren.

> ☛ *Sie können eine Entität mit einem Konto im Abschnitt **Umfang** des Kontos verbinden.*

Folgende Merkmale für ein Konto sind verfügbar:

- **Kontotyp**
  Das Konto der Gewinn- und Verlustrechnung beschreibt den Aufwand und die Erträge des Unternehmens während des betroffenen Geschäftsjahres. Sie können den Kontotyp angeben:
  - "Gewinne"
  - "Verluste"
- **Gesamtwert**: Sie können für dieses Konto einen Betrag eingeben.

  > ☛ *Eine Größenordnung kann ausreichen.*
- **Status**
  - "Geöffnet": Das Konto ist aktiv
  - "Geschlossen": Das Konto ist inaktiv

  > ☛ *Das Konto kann aus mehreren Konten bestehen.*

  > ☛ *Dieser Objekttyp ist in der Lösung **HOPEX IT Risk Management** nicht verfügbar.*

RESSOURCEN DES UNTERNEHMENS

Die globale Beschreibung der Architektur des Informationssystems eines Unternehmens kann beschränkt werden und nur Server aufführen sowie die Anwendungen und Datenbanken aufführen, die für diesen Informationsaustausch sorgen.

> ☛ *Diese Navigationsregisterkarte ist in der Lösung **HOPEX IT Risk Management** nicht verfügbar. Um in dieser Lösung die Beschreibungen der Anwendungen zu erhalten, siehe Navigationsregisterkarte **Bibliothek**.*

So kann die Beschreibung des Kontextes, in dem ein Risikomanagementprojekt durchgeführt wird, auch mit folgender Beschreibung ergänzt werden:

- Anwendungen

  > 🕮 *Eine Anwendung besteht aus Software-Komponenten, die im Rahmen der IT-Entwicklungen eine konsistente Einheit bilden.*

- Datenbanken

  > 🕮 *Eine Datenbank ermöglicht, die logische oder physische Archivierungsstruktur der Daten anzugeben.*

- Server der Datenbanken und Anwendungen

  > 🕮 *Ein Server ist eine Hardware-Ressource, die über eine Datenbank verfügen kann, auf der eine Anwendung ausgeführt werden kann.*

Um Zugriff auf die IT-Ressourcen zu erhalten, gehen Sie wie folgt vor:

❱ Klicken Sie im Desktop **Umgebung** auf **Ressourcen**.

Um beispielsweise die Merkmale einer Anwendung zu definieren, gehen Sie wie folgt vor:

1. Klicken Sie in der Baumstruktur der Ressourcen links neben der Bearbeitungszone auf **Anwendung**.
   Die Baumstruktur der Anwendungen wird in der Bearbeitungszone angezeigt.
2. Klappen Sie den Ordner **Anwendungen** auf.
   Nun wird die Liste der Anwendungen angezeigt.
3. Wählen Sie eine Anwendung aus.
   Die Eigenschaftsseite wird rechts neben der Bearbeitungszone angezeigt.

> ☛ *Genauso können Sie die Merkmale der Objekte **Server** und **Datenbank** anzeigen.*

Die Anwendungen

Sie können im Eigenschaftsfenster der Anwendung im Abschnitt **Umfang** viele Objekte verbinden:

- Geschäftssparte

  > 🕮 *Eine Geschäftssparte ist eine Kompetenz oder eine Gruppierung von Kompetenzen im Interesse des Unternehmens. Sie entspricht zum*

Beispiel großen Produktsegmenten oder Distributionskanälen bzw. Geschäftstätigkeiten.

- Geschäftsprozess

  Ein Geschäftsprozess stellt ein System dar, das Produkte oder Dienstleistungen an einen internen oder externen Kunden des Unternehmens oder Organisation liefert. Auf höherer Ebene definiert ein Geschäftsprozess eine Strukturierung und Kategorisierung des Geschäftsbereichs eines Unternehmens. Der Geschäftsprozess kann in weitere Prozesse unterteilt werden. Mit der Verbindung zu den organisatorischen Prozessen kann die reelle Implementierung des Geschäftsprozesses in der Organisation beschrieben werden. Ein Geschäftsprozess kann auch mit einer funktionalen Sicht detailliert werden.

- Risiko

  Ein Risiko ist eine mehr oder weniger wahrscheinliche Gefahr, der eine Organisation ausgesetzt ist.

- Kontrolle

  Eine Kontrolle ist ein Mittel, ein oder mehrere Risiken unter Kontrolle zu haben, und sicherzustellen, dass eine gesetzliche, vorschriftsmäßige, strategische oder interne Anforderung des Unternehmens erfüllt wird.

- Kontrollsystem

  Ein Kontrollsystem besteht aus mehreren Kontrollen, mit denen Risiken für ein Unternehmen verhütet und Risiken unter Kontrolle gehalten werden können, sowie interne Betriebsregeln angewendet, Gesetze oder Vorschriften eingehalten oder strategische Ziele des Unternehmens erreicht werden können.

  ☛ *Nicht in **HOPEX IT Risk Management** verfügbar.*

- Aktionsplan

  Ein Aktionsplan besteht aus einer Reihe von Aktionen mit dem Ziel, Risiken und Ereignisse zu reduzieren, die sich auf die Aktivität eines Unternehmens auswirken können.

- Vorfälle

  Ein Vorfall ist ein Fakt einer internen oder externen Quelle, der sich auf die Organisation auswirkt. Er bildet das Grundelement für die Sammlung von Daten über ein Betriebsrisiko.

Im Lesezugriff können Sie folgende Objekte folgender Typen aufrufen:

- Problem
- Geschäftsfähigkeit
- Implementierte Funktionalität

Sie können zum Beispiel angegeben, welche Anwendung einer Entität zur Verfügung gestellt oder bei der Ausführung eines Prozesses verwendet wird.

Datenbanken und Server

Sie können angeben:

- auf welchem Server die Datenbanken installiert werden
- von welchen Entitäten sie verwendet werden
- von welchen Prozessen sie aufgerufen und aktualisiert werden

Bei der Erfassung einer Bestellung ruft der Vertriebsmitarbeiter die Kundendatenbank des Sitzes auf und aktualisiert die Vertriebsdatenbank der Zweigstelle.

☛ *Diese Objekttypen sind in der Lösung **HOPEX IT Risk Management** nicht verfügbar.*

RACI

MEGA ermöglicht, die Verantwortungen der Prozesse in der RACI-Kreuztabelle zu definieren.

☛ *RACI steht als Akronym für Responsible (Durchführungsverantwortlicher), Accountable (Rechenschaftspflichtiger), Consulted (Konsultiert), Informed (Informiert).*

Verantwortungsstufen

Folgende Stufen werden vorgeschlagen:

Verantwortung	Erklärung
Durchführungsver-antwortlicher	Person, die für die Durchführung der geplanten Aktionen zuständig ist.
Rechenschaftspflich-tig	Person, die über den Fortschritt der geplanten Aktionen berichtet und Entscheidungen trifft. Es gibt jeweils nur einen "Rechenschaftspflichtigen" pro Aktion.
Konsultiert	Person, die vor einer Aktion oder einer Entscheidung als Erste zu Rate gezogen wird.
Informiert	Person, die nach einer Aktion oder Entscheidung informiert werden muss.

MEGA ermöglicht, die Verantwortungsstufe der einzelnen Personen anzugeben:

- für einen Geschäftsprozess und einen organisatorischen Prozess
- für ein Risiko
- für eine Kontrolle

Verantwortungen angeben

Für die Lenkung eines Objekts können eine oder mehrere Personen verantwortlich sein.

Um die von einem Objekt betroffenen Personen anzugeben, gehen Sie wie folgt vor:

1. Klappen Sie in der Eigenschaftsseite des Objekts den Abschnitt **RACI** auf.

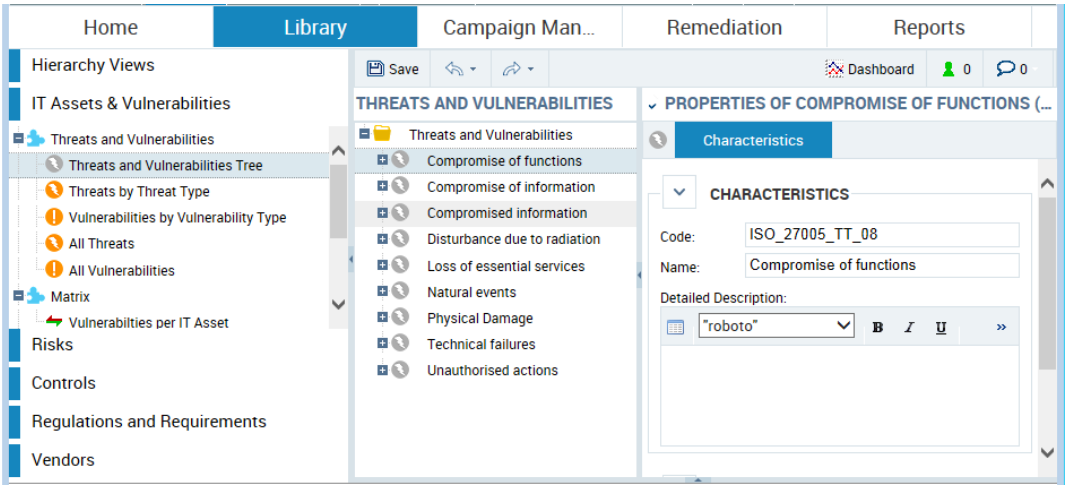
2. Verbinden Sie Personen oder Zuweisungen von Personen in folgenden Registerkarten:
   - **Durchführungsverantwortlicher**
   - **Rechenschaftspflichtig**
   - **Konsultiert**
   - **Informiert**.

   ☛ *In bestimmten Lösungen können sich die RACI-Informationen mit bestimmten und an anderer Stelle definierten Rollen im Eigenschaftsfenster des Objekts wiederholen oder sie aber ergänzen.*

   Zum Beispiel muss der Durchführungsverantwortliche des Prozesses in **HOPEX ERM** direkt im Eigenschaftsfenster des Prozesses im Feld **Durchführungsverantwortlicher** und nicht im RACI-Abschnitt angegeben werden. In diesem Fall ist es also wichtig, nur einen Durchführungsverantwortlichen anzugeben.

BIBLIOTHEK VERWENDEN

In der Bibliothek IT RM (IT Risk Management) kann der Bestand der Elemente aufgerufen und aufgestellt werden, die für das Management von IT-Risiken, IT-Compliance und IT-Anbietern notwendig sind.



✓ "Bestand der IT-Assets", Seite 56
✓ "Bestand der Bedrohungen und Anfälligkeiten", Seite 61
✓ "Bestand der Risiken und Kontrollen", Seite 66
✓ "Bestand der Anforderungen und Vorschriften", Seite 69
✓ "Bestand der Anbieter", Seite 70

☛ *Weitere Informationen zur Verwendung der Bibliothek finden Sie unter "HOPEX IT Risk Management benutzen", Seite 71.*

BESTAND DER IT-ASSETS

Über den Bestand der IT-Assets

Ein IT Asset ist ein Softwareartefakt (Beispiel: Anwendung, Softwaretechnologie) oder Hardwareartefakt (Beispiel: Standort, Server), das vom Unternehmen gehalten und im Rahmen seiner Geschäftstätigkeiten verwendet wird.

Es gibt zwei Familien von IT Assets:

- IT Asset (Typ)

  ☛ *Ein Asset-Typ ist eine spezifische Kategorie des IT-Assets, die Objekttypen (Anwendung, Softwaretechnologie usw.) gruppiert, im Gegensatz zu den bereitgestellten Objekten (Instanzen).*

- IT Asset (Instanz)

  ☛ *Eine Asset-Instanz ist ein spezifischer Typ des IT-Assets, der die Objekte einer Bereitstellung gruppiert (Softwareinstallation und bereitgestellte Technologie).*

Bestand des IT-Assets aufstellen

Bei der Verwaltung des IT-Assets werden zunächst die IT-Assets eines Unternehmens identifiziert und beschrieben. Erst wenn Sie alle Assets ermittelt haben, können sie effizient kontrolliert und verwaltet werden.

Die Verwaltung von IT-Assets ist wichtig, sowohl in finanzieller als auch in operativer Hinsicht. Denn durch eine gute Verwaltung lassen sich die Ressourcen optimieren und Risiken in puncto Compliance und Sicherheit reduzieren.

Typen von IT-Assets

Ein Asset-Typ ist eine Asset-Kategorie, die Objekttypen (Anwendung, Software, Technologie) gruppiert, im Gegensatz zu den bereitgestellten Objekten, die Instanzen genannt werden.

Sie können unterscheiden:

- Assets
  - Anwendung

    ☛ *Eine Anwendung besteht aus Software-Komponenten, die im Rahmen der IT-Entwicklungen und Funktionalitäten für die Benutzer eine konsistente Einheit bilden.*

  - Technologie

    ☛ *Eine Softwaretechnologie ist eine Grundkomponente, die für Geschäftsanwendungen notwendig ist.*

- Bereitgestellte Assets:
  - Softwareinstallation

    ☛ *Eine Softwareinstallation stellt die Bereitstellung einer Anwendung dar, die an einem bestimmten Standort verwendet werden soll.*

  - Bereitgestellte Technologie

Anwendungen beschreiben

Um auf die Merkmale zuzugreifen, mit denen eine Anwendung identifiziert werden kann, gehen Sie wie folgt vor:

❱ Klicken Sie in den Eigenschaftsseiten einer Anwendung auf die Registerkarte **Merkmale**.

Allgemeine Merkmale der Anwendung

Dort können Sie angeben:

- den **Namen** der Anwendung
- den internen **Code**

Anwendungstyp

Es kann mehrere Typen von Technologien geben:

- Büroautomation
- spezifische Entwicklung
- Middleware
- Softwareprogrammpaket
- System

Funktionaler Umfang der Anwendung.

Um die Objekte aufzurufen, die die funktionale Abdeckung einer Anwendung definieren, gehen Sie wie folgt vor:

❱ Klicken Sie in den Eigenschaftsseiten der Anwendung auf **Merkmale** und anschließend auf **Funktionaler Umfang**.

Die Datentypen, die die funktionale Abdeckung definieren, sind:

- Die Geschäftssparten, die die Anwendung verwenden

  📖 *Eine Geschäftssparte ist eine hohe Klassierungsebene der wichtigsten Geschäftstätigkeiten eines Unternehmens. Sie entspricht zum Beispiel großen Produktsegmenten oder Distributionskanälen. Sie ermöglicht, Prozesse eines Unternehmens, organisatorische Einheiten oder Anwendungen für ein bestimmtes Produkt und/oder einen bestimmten Markt zu klassieren. Regelwerke bestimmter Industrien schreiben ihre eigenen Listen von Geschäftssparten vor.*

- Die Geschäftsprozesse , die die Anwendung verwenden

  📖 *Ein Geschäftsprozess stellt ein System dar, das Produkte oder Dienstleistungen an einen internen oder externen Kunden des Unternehmens oder Organisation liefert. Auf höherer Ebene definiert ein Geschäftsprozess eine Strukturierung und Kategorisierung des Geschäftsbereichs eines Unternehmens. Der Geschäftsprozess kann in weitere Prozesse unterteilt werden. Mit der Verbindung zu den organisatorischen Prozessen kann die reelle Implementierung des Geschäftsprozesses in der Organisation beschrieben werden. Ein*

Geschäftsprozess kann auch mit einer funktionalen Sicht detailliert werden.

☛ *Weitere Informationen zur Liste der verfügbaren Geschäftsprozesse finden Sie unter "Geschäftsprozesse definieren", Seite 29.*

- Die Geschäftsfähigkeiten, die von der Anwendung abgedeckt werden.

  🕮 *Eine Geschäftsfähigkeit ist eine Einheit zur Aufteilung der Bearbeitungen eines Informationssystems. Bei den Bearbeitungen kann es sich zum Beispiel um die Tätigkeit oder den Geschäftsbereich eines Unternehmens handeln.*

Verantwortungen hinsichtlich einer Anwendung

Lokaler Eigentümer einer Anwendung

Der Eigentümer einer Anwendung ist während des gesamten Lebenszyklus dieser Anwendung für die Verwaltung der Anwendung verantwortlich. Er muss sicherstellen, dass die Anwendung richtig beschrieben wird.

☛ *Der Begriff "Eigentümer" identifiziert eine Person oder eine Entität, die die Verantwortung für die Entwicklung, Wartung und Verwendung der Assets akzeptiert. Dieser Begriff bedeutet nicht, dass die Person Eigentumsrechte für die Assets hat.*

Um einen oder mehrere Eigentümer anzugeben, gehen Sie wie folgt vor:

1. Klappen Sie in der Eigenschaftsseite der Anwendung den Abschnitt **Verantwortungen** auf.
2. Wählen Sie die Registerkarte **Lokaler Eigentümer einer Anwendung** aus und verbinden Sie einen oder mehrere Benutzer.

Local IT Risk Manager

Der "Local IT Risk Manager" ist der lokale Ansprechpartner des Risikos auf der Ebene der Anwendungen.

☛ *Die mit einem Local IT Risk Manager oder dem lokalen Eigentümer einer Anwendung verbundenen Anwendungen werden in der Registerkarte **Home** unter **Meine Verantwortungen > Meine IT-Assets** aufgeführt.*

Mit den Anwendungen verbundene Technologien

Ab der Eigenschaftsseite einer Anwendung können Sie existierende Technologien verbinden oder neue Technologien erstellen.

Um ab einer Anwendung auf Technologien zuzugreifen, gehen Sie wie folgt vor:

❱ Klappen Sie im Eigenschaftsfenster einer Anwendung den Abschnitt **Technologien** auf.

Ausgetauschte Daten

Diese Informationen stammen aus **MEGA IT Portfolio Management**:

Die *Nachrichtenflüsse*, ihre Richtung und ihr Inhalt, der unter den Anwendungen ausgetauscht wird, können beschrieben werden. Mit diesen Informationen wird eine Kartografie über den Austausch erstellt.

> 🕮 *Ein Nachrichtenfluss stellt einen Informationsfluss innerhalb des Unternehmens oder zwischen dem Unternehmen und seiner Umgebung dar. Ein Nachrichtenfluss kann einen Inhalt transportieren.*

Der Inhalt eines Nachrichtenflusses wird mit Geschäftsdaten dargestellt.

> 🕮 *Geschäftsdaten bezeichnen den Inhalt eines Nachrichtenflusses. Geschäftsdaten können von mehreren Nachrichtenflüssen verwendet werden, da sie nicht mit einem Sender oder einem Empfänger verknüpft sind. Dieselben Geschäftsdaten können von mehreren Nachrichtenflüssen verwendet werden.*

Anfälligkeiten einer Anwendung

Um die Anfälligkeiten einer Anwendung aufzurufen, gehen Sie wie folgt vor:

- Wählen Sie im Eigenschaftsfenster der Anwendung die Registerkarte **IT-Risiken** aus und klappen Sie anschließend den Abschnitt **Anfälligkeiten** auf.

Mit einer Anwendung verbundene Kontrollen

Um die Kontrollen hinsichtlich einer Anwendung aufzurufen, gehen Sie wie folgt vor:

- Wählen Sie im Eigenschaftsfenster der Anwendung die Registerkarte **Kontrollen** aus.

Softwareinstallationen

Softwareinstallationen sind Anwendungen, die an Standorten bereitgestellt werden.

Um auf Softwareinstallationen zuzugreifen, gehen Sie wie folgt vor:

- Klicken Sie auf **Bibliothek > Hierarchische Ansichten > Bereitgestellte Anwendungen**.
  Die Softwareinstallationen sind nach Standorten klassiert.

Technologien beschreiben

> 🕮 *Eine Technologie ist eine Definition oder ein Format, das von einer Normungsorganisation zugelassen wurde oder von der Industrie als Standard akzeptiert wird.*

Zugriff auf die Techologien

Um auf die Liste aller Technologien zuzugreifen, gehen Sie wie folgt vor:

- Klicken Sie auf **Bibliothek > IT-Assets > Alle Technologien**.

Merkmale einer Technologie definieren

Um die technischen Merkmale einer Technologie anzugeben, gehen Sie wie folgt vor:

1. Klicken Sie in den Eigenschaftsseiten einer Anwendung auf **Merkmale** und anschließend auf **Technologie**.

Sie können das Feld **Identifizierung** der Technologie angeben:

- den **Namen** der Technologie
- den internen **Code**
- den **Anbieter**

Technologietypen

Sie können den **Technologietyp** angeben:

- IT-Services
- Betriebssystem
- Plattform
- RDBMS

Eine Technologie kann mit einem oder mehreren Technologietypen verbunden werden.

☛ *Nur der funktionale Administrator kann neue Technologietypen erstellen.*

Risiken und Anfälligkeiten einer Technologie

Sie können die Technologie auch mit folgenden Elementen verbinden:

- Risiken
- Anfälligkeiten

🕮 *Anfälligkeiten sind Fehler in der Kontrolle eines (IT) Assets, die sie auf eine Bedrohung anfällig machen und zu Mängeln beim Datenschutz, bei der Vollständigkeit oder der Verfügbarkeit dieses Assets führen können.*

BESTAND DER BEDROHUNGEN UND ANFÄLLIGKEITEN

Beispiele von Bedrohungen, Anfälligkeitstypen und Anfälligkeiten

Anfälligkeitstypen	Anfälligkeiten	Bedrohungen
Hardware	Anfällig auf Temperatur-schwankungen	Meteorologisches Ereignis
Hardware	Nicht gesicherte Lagerung	Daten- oder Dokumenten-diebstahl
Software	Komplizierte Benutzerober-fläche	Bedienungsfehler
Netzwerk	Nicht gesichertes Kennwort	Nicht erlaubter Zugriff
Persönlich	Keine Richtlinien für die Soft-warenutzung	Nicht erlaubte Softwarenut-zung
Standort	Hardware in einem über-schwemmungsgefährdeten Gebiet	Überschwemmung

Beispiele aus der Norm ISO 27005:2011

Alle Bedrohungen

Bedrohungen sind externe oder interne Faktoren, die (IT) Assets des Unternehmens gefährden Jede Bedrohung gruppiert mehrere Anfälligkeiten. Weitere Informationen finden Sie unter "Anfälligkeiten aufrufen", Seite 62.

Zugriff auf Bedrohungen

Um auf Bedrohungen zuzugreifen, gehen Sie wie folgt vor:

- Klicken Sie auf **Bibliothek > Bedrohungen und Anfälligkeiten > Alle Bedrohungen**.

  ☛ *Sie können auf die Bedrohungen auch nach Bedrohungstyp zugreifen. Siehe "Merkmale der Bedrohungen", Seite 62.*

Bedrohungstyp erstellen

Um einen Bedrohungstyp zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie auf **Bibliothek > IT Assets & Anfälligkeiten > Bedrohungen und Anfälligkeiten > Baumstruktur der Bedrohungen und Anfälligkeiten**.
2. Klicken Sie mit der rechten Maustaste auf den Stamm der Baumstruktur "Bedrohungen und Anfälligkeiten" und wählen Sie anschließend **Neu > Bedrohungstyp** aus.
   Der neue Bedrohungstyp wird in der Baumstruktur angezeigt.

Merkmale der Bedrohungen

Sie können:

- den Bedrohungsytp angeben, dem die Bedrohung angehört

  📖 *Mit den Bedrohungstypen lassen sich die Bedrohungen nach verschiedenen Kategorien gruppieren (Beispiel: Körperschaden, Naturereignisse, technische Fehler usw.). Für die Erstellung siehe "Bedrohungstyp erstellen", Seite 62*

- die Anfälligkeiten mit der Bedrohung im entsprechenden Abschnitt verbinden

  ☛ *Anfälligkeiten sind Fehler in der Kontrolle eines (IT) Assets, die sie auf eine Bedrohung anfällig machen und zu Mängeln beim Datenschutz, bei der Vollständigkeit oder der Verfügbarkeit dieses Assets führen können.Weitere Informationen finden Sie unter "Anfälligkeiten aufrufen", Seite 62.*

Anfälligkeiten aufrufen

Anfälligkeiten sind Fehler in der Kontrolle eines (IT) Assets, die sie auf eine Bedrohung anfällig machen und zu Mängeln beim Datenschutz, bei der Vollständigkeit oder der Verfügbarkeit dieses Assets führen können.

Die Anfälligkeiten können aus den nationalen Datenbanken oder Managementtools für Anfälligkeiten importiert werden.

Zugriff auf Anfälligkeiten

Um auf Anfälligkeiten zuzugreifen, gehen Sie wie folgt vor:

❱ Klicken Sie auf **Bibliothek > Bedrohungen und Anfälligkeiten > Alle Anfälligkeiten**.

☛ *Sie können auf die Anfälligkeiten auch nach Anfälligkeitstyp zugreifen. Siehe "Quelle", Seite 63.*

Anfälligkeitstyp erstellen

Um einen Anfälligkeitstyp zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie auf **Bibliothek > IT Assets & Anfälligkeiten > Bedrohungen und Anfälligkeiten > Anfälligkeiten nach Anfälligkeitstyp**.

2. Klicken Sie mit der rechten Maustaste auf den Stamm der Baumstruktur "Anfälligkeiten" und wählen Sie anschließend **Neu > Anfälligkeitstyp** aus.
   Der neue Anfälligkeitstyp wird in der Baumstruktur angezeigt.

Merkmale der Anfälligkeiten

Bedrohung

Es handelt sich um die Bedrohung, die die Anfälligkeit potenziell nutzt.

☛ *Eine Anfälligkeit kann nur auf eine einzige Bedrohung zurückgeführt werden.*

Anfälligkeitstyp

Anfälligkeitstypen gruppieren Anfälligkeiten nach verschiedenen Kategorien (Beispiel: Software, Organisationen, (geografischer) Standort usw.).

☛ *Um einen Typ zu erstellen, siehe "Anfälligkeitstyp erstellen", Seite 62.*

Datum der ersten Veröffentlichung

Das Datum der Veröffentlichung entspricht dem Datum, an dem die Anfälligkeit zum ersten Mal beschrieben wurde.

Dieses Merkmal ist optional. Es kann für den Import aus der Quelle eines Dritten nützlich sein.

Letztes Änderungsdatum

Das letzte Änderungsdatum entspricht dem Datum, an dem die Anfälligkeit geändert wurde.

Dieses Merkmal ist optional. Es kann für den Import aus der Quelle eines Dritten nützlich sein.

Quelle

Die Anfälligkeiten werden von nationalen Organismen oder Normungsanstalten zur Verfügung gestellt und regelmäßig aktualisiert. Beispiel:

- NIST (National Institute of Standards and Technology)
- CVE (Common Vulnerabilities and Exposures)
- ISO (ISO 27000)

Status

- Potenzial
- Ermittelt
- Bearbeitet
- Geschlossen

Anfälligskeits-Score

- Schwach
- Mittel
- Erhöht

Umfang der Anfälligkeiten

Der Umfang der Anfälligkeiten setzt sich aus zwei Abschnitten zusammen:

- Assets
- Bereitgestellte Assets

> ☛ *In der Praxis wird je nach verfügbarem Bestand (Typen oder Bereitstellungen) entweder die eine oder die andere Verbindung verwendet.*

Anfällige IT Assets

- Anwendungen

> 🕮 *Eine Anwendung besteht aus Software-Komponenten, die im Rahmen der IT-Entwicklungen und Funktionalitäten für die Benutzer eine konsistente Einheit bilden.*

- Softwaretechnologie

> 🕮 *Eine Softwaretechnologie ist eine Grundkomponente, die für Geschäftsanwendungen notwendig ist.*

Bereitgestellte anfällige IT Assets

- Softwareinstallation

> 🕮 *Eine Softwareinstallation stellt die Bereitstellung einer Anwendung dar, die an einem bestimmten Standort verwendet werden soll.*

- Bereitgestellte Technologie

> 🕮 *Eine Softwaretechnologie ist eine Grundkomponente, die für Geschäftsanwendungen notwendig ist.*

Umfang der Anfälligkeiten definieren

Mit einer Kreuztabelle können Sie IT-Assets und Anfälligkeiten schnell verbinden.

Um auf diese Kreuztabelle zuzugreifen, gehen Sie wie folgt vor:

1. Klicken Sie auf **Bibliotheken > IT-Assets und Anfälligkeiten > Kreuztabelle > Anfälligkeit nach IT-Asset**.

CVSS-Bewertung

Common Vulnerability Scoring System (CVSS) ist ein standardisiertes Bewertungssystem für die Kritizität der Anfälligkeiten mit objektiven und messbaren Kriterien.

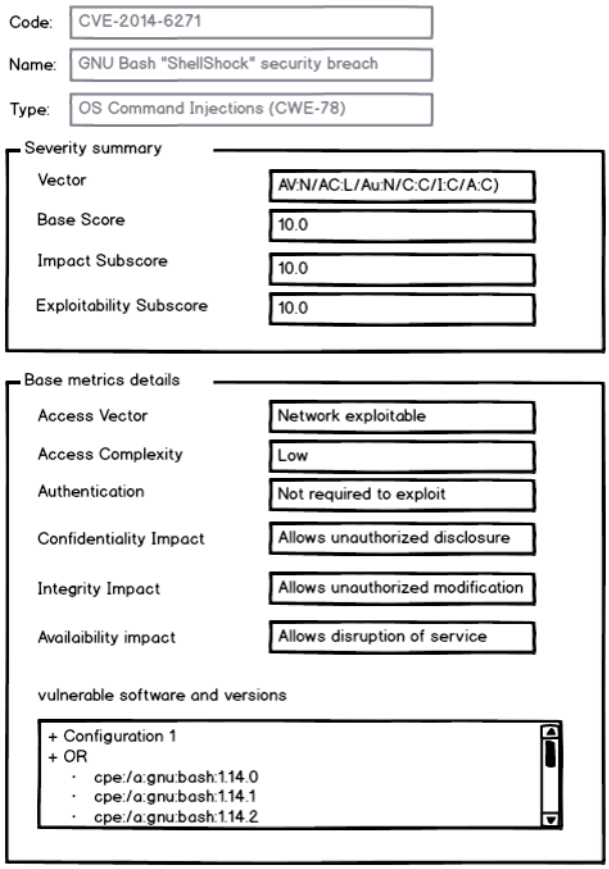
CVSS ist eine Notation des NIST (National Institue of Standards and Technology) in den USA und ein Standard.

> ☛ *Diese Daten werden aus Systemen Dritter importiert und können in **HOPEX IT Risk Management** nicht eingegeben werden.*

Datenbeispiele

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-6461

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-6461



Berichte über die Anfälligkeiten

Die Anfälligkeiten werden anhand verschiedener Berichte veranschaulicht. Siehe "Berichte über die Anfälligkeiten", Seite 132.

BESTAND DER RISIKEN UND KONTROLLEN

Risiken aufrufen

Zugriff auf die Risiken

Um auf die Risiken zuzugreifen, gehen Sie wie folgt vor:

❱ Klicken Sie auf **Bibliothek > Risiken > Alle Risiken**.

Sie können auch auf folgende Elemente zugreifen:

- Hauptrisiken

  ☛ *Hauptrisiken sind Risiken, bei denen im Eigenschaftsfenster des Risikos das Kästchen Hauptrisiko markiert wurde.*

- Risiken, die nicht mit einer Kontrolle verbunden sind

Bewertete Merkmale

Auswirkung

Eine Auswirkung beschreibt die Auswirkung des Risikos, wenn das Risiko auftritt.

Wahrscheinlichkeit

Die Wahrscheinlichkeit, dass das Risiko auftritt.

Inhärentes Risiko

Ein Bruttorisiko bezeichnet ein Risiko für ein Unternehmen, wenn keine Maßnahmen getroffen werden, die Wahrscheinlichkeit oder Auswirkung dieses Risikos zu ändern. Es handelt sich um den Wert der Auswirkung, der vom Wert der Wahrscheinlichkeit produziert wurde, bevor Präventionsmaßnahmen oder Maßnahmen zur Risikominderung berücksichtigt werden.

Demnach ist ein inhärentes Risiko = Auswirkung * Wahrscheinlichkeit

Geschwindigkeit

Die Geschwindigkeit stellt dar, wie schnell sich ein Risiko ab einem Asset bei einem Vorfall auf andere Assets ausweitet. Die Geschwindigkeit ist ein Mittel, das Risiko zu beschreiben (anders als mit der Auswirkung und der Häufigkeit).

Gewichtetes inhärentes Risiko

Inhärentes Risiko * Geschwindigkeit

Umfang des Risikos

Im Eigenschaftsfenster eines Risikos können Sie identifizieren:

- riskante IT-Assets
  - Anwendungen

    Eine Anwendung besteht aus Software-Komponenten, die im Rahmen der IT-Entwicklungen und Funktionalitäten für die Benutzer eine konsistente Einheit bilden.
  - Softwaretechnologien

    Eine Softwaretechnologie ist eine Grundkomponente, die für Geschäftsanwendungen notwendig ist.
- Bereitgestellte riskante Assets
  - Softwareinstallationen

    Eine Softwareinstallation stellt die Bereitstellung einer Anwendung dar, die an einem bestimmten Standort verwendet werden soll.
  - Bereitgestellte Technologien

    Eine Softwaretechnologie ist eine Grundkomponente, die für Geschäftsanwendungen notwendig ist.

Um den Umfang eines Risikos anzugeben, gehen Sie wie folgt vor:

1. Klicken Sie im Eigenschaftsfenster des Risikos je nach Bedarf folgenden Abschnitt auf:
   - **Umfang (riskantes IT-Asset)**, oder
   - **Umfang (bereitgestelltes riskantes IT-Asset)**

     ☛ *Die Definition des Risikoumfangs wirkt sich auf die direkten Bewertungen aus.*
2. Verbinden Sie die betroffenen Objekte.

   ☛ *Weitere Informationen zum Umfang der Risiken finden Sie unter "Der Umfang eines Risikos", Seite 37.*

Analyse des Risikos

Weitere Informationen finden Sie unter "Analyse eines Risikos", Seite 38.

Bewertung des Risikos

Die Bewertung des Risikos kann erfolgen nach:

- Anwendung
- bereitgestellter Anwendung (oder Installation)

  ☛ *Die im Eigenschaftsfenster des Risikos verfügbare Registerkarte hängt von der Wahl ab, die hinsichtlich der Risikobewertung getroffen wurde.*

Weitere Informationen finden Sie unter "So genannte Experten-Risiken bewerten", Seite 78.

Bearbeitung des Risikos

Weitere Informationen finden Sie unter "Umzusetzende Kontrollen und Aktionen angeben", Seite 111.

Kontrollen aufrufen

Eine Kontrolle ist ein Mittel, ein oder mehrere Risiken unter Kontrolle zu haben, und sicherzustellen, dass eine gesetzliche, vorschriftsmäßige oder interne Anforderung des Unternehmens erfüllt wird.

Eine falsch implementierte Kontrolle kann eine Anfälligkeit darstellen.

Zugriff auf die Kontrollen

Um auf die Kontrollen zuzugreifen, gehen Sie wie folgt vor:

❱ Klicken Sie auf **Bibliothek > Kontrollen > Alle Kontrollen**.

Im Eigenschaftsfenster eines Kontrolltyps können Sie Kontrollen verbinden.

Umfang einer Kontrolle

Im Rahmen von **HOPEX IT Risk Management** können Sie mehrere Objekttypen mit einer Kontrolle verbinden.

Sie können verbinden:

- Die im Standardumfang einer Kontrolle enthaltenen Objekttypen: siehe "Der Umfang einer Kontrolle", Seite 41
- Anwendungen (Abschnitt **Umfang (IT-Assets)**).

Bewertung der Kontrollen

Im Eigenschaftsfenster einer Kontrolle kann in der Registerkarte **Bewertung** eine direkte Bewertung ab der Bewertungsvorlage "Bewertung der Kontrollen nach Anwendung" vorgenommen werden.

Siehe "Kontrollen von Experten bewerten", Seite 82.

Arbeitsumgebung für Fragebögen vorbereiten

Bevor Sie eine Bewertungskampagne starten, müssen Sie die Arbeitsumgebung vorbereiten. Folgende Schritte müssen Sie zuvor durchführen:

- Risiken/Kontrollen mit Anwendungen verbinden

  ☛ *Weitere Informationen finden Sie unter "Risiken auf IT-Assets positionieren", Seite 73.*

  ☛ *Um stichhaltige Berichte zu erhalten, kann es nützlich sein, Anwendungen mit Prozessen, Geschäftssparten oder Geschäftsfähigkeiten zu verbinden. Dieser Schritt ist jedoch nicht notwendig, um Bewertungskampagnen zu starten.*

- lokalen Anwendungseigentümer für jede Anwendung definieren

  ☛ *Ausführliche Informationen finden Sie unter "Verantwortungen hinsichtlich einer Anwendung", Seite 58.*

Weitere Informationen zu den Bewertungen finden Sie unter "Bewertungen mit Fragebögen", Seite 87.

BESTAND DER ANFORDERUNGEN UND VORSCHRIFTEN

Um auf die Anforderungen und Vorschriften zuzugreifen, gehen Sie wie folgt vor:

❱ Klicken Sie auf **Bibliothek > Anforderungen und Vorschriften**.
Die Baumstruktur der Vorschriften und Anforderungen wird angezeigt.

Merkmale der Vorschriften

> 🕮 *Eine Vorschrift oder ein Regelwerk stellt mehrere Richtlinien mit oder ohne Bedingungen auf, die von der Regierung im Rahmen eines Gesetzes, von einem Berufsverband in Form von Best Practices oder intern von einer Organisation festgelegt werden.*

Weitere Informationen finden Sie unter "Merkmale einer Vorschrift", Seite 43.

Im Eigenschaftsfenster einer Vorschrift können Sie verbinden:

- Geschäftsprozesse (im Abschnitt **Umfang**)
- Untervorschriften
- Anforderungen

Merkmale von Anforderungen

> 🕮 *Eine Anforderung ist ein explizit ausgedrückter Bedarf oder eine Erwartung, die wie eine Einschränkung vorgeschrieben und im Rahmen eines Zertifikations-, Organisations- oder Modifikationsprojekts für das Informationssystem des Unternehmens erfüllt werden muss.*

Weitere Informationen finden Sie unter "Merkmale der Anforderungen", Seite 46.

Um den Parameter einer Anforderung anzugeben, gehen Sie wie folgt vor:

❱ Klicken Sie im Eigenschaftsfenster der Anforderung auf die Registerkarte **Umfang**.
Im Abschnitt **Beitragsleistende Elemente** können Sie angeben:

- **Kontrolltypen**

  > ☛ *Mit einem Kontrolltyp lassen sich die Kontrollen klassieren, die im Unternehmen entsprechend des Standards bzw. Normen der betreffenden Sektoren oder Vorschriften/Reglementierungen (Cobit usw.) implementiert sind.*

- **Kontrollen**

Bestand der Anbieter

Bei den IT-Anbietern kann es sich um Softwareunternehmen oder andere Dienstleister handeln.

Zugriff auf die Liste der Anbieter

Um auf die Liste der Anbieter zuzugreifen, gehen Sie wie folgt vor:

- Klicken Sie auf **Bibliothek > Anbieter > Alle Anbieter**.

Merkmale der Anbieter

Anbietertyp

Ein Anbieter ist eine Entität vom Typ "Anbieter".

Reporting

Siehe "Kosten von Produkten und Services angeben", Seite 84.

Informationen der Fakturierung

- Firmenname
- Handelsname des Anbieters: gebräuchlicher Name, wenn der Name nicht dem Firmennamen entspricht (Englisch: DBA, Doing Business As)
- Rechnungsadresse des Lieferanten
- Telefon

Informationen über den Hauptkontakt

- Name
- Adresse
- E-Mail
- Titel: Position (beispielsweise Account Manager)

Liste der angebotenen Technologien

Im Eigenschaftsfenster des Anbieters können Sie die Liste der angebotenen Technologien aufrufen.

Bewertung des Anbieterrisikos

In dieser Registerkarte können Sie dem Anbieter eine Note geben. Weitere Informationen finden Sie unter "Anbieter bewerten", Seite 85.

Die Fragebögen zur Bewertung des Anbieters werden hier ebenfalls aufgeführt.

HOPEX IT Risk Management benutzen

Sobald die Bibliothek der IT-Assets erstellt ist, können sie mit **HOPEX IT Risk Management** IT-Risiken verwalten. Die Lösung erlaubt ebenfalls, IT-Compliance und IT-Anbieter zu verwalten.

- ✓ "IT-Risiken verwalten", Seite 72
- ✓ "IT-Compliance verwalten", Seite 80
- ✓ "IT-Anbieter verwalten", Seite 84

IT-RISIKEN VERWALTEN

Wenn Sie den IT-Bestand Ihres Unternehmens aufgestellt haben, können Sie im Anschluss:

- Anfälligkeiten der IT-Assets positionieren
- Risiken identifizieren
- Risiken bei IT-Assets positionieren
- Risikoszenarios identifizieren
- Risiken von so genannten Experten oder über Bewertungskampagnen bewerten
- Aktionspläne für eine Verbesserung definieren

Weitere Informationen zu den Merkmalen von Risiken finden Sie unter "Risiken aufrufen", Seite 66.

Sie können jederzeit Berichte über die Verwaltung von IT-Risiken, Bedrohungen und Anfälligkeiten generieren. Weitere Informationen finden Sie unter "Berichte über IT-Risiken", Seite 124.

IT- und Softwarebestand aufstellen

Um die Risiken zu verwalten, müssen die Assets klar identifiziert und im Anschluss ein Bestand aller Assets aufgestellt und verwaltet werden.

☛ *Weitere Informationen finden Sie unter "Bestand der IT-Assets", Seite 56.*

Anfälligkeiten auf IT-Assets positionieren

Sie können die Anfälligkeiten identifizieren und mit den Assets verbinden (Anwendung oder Softwaretechnologie). Diese Aufgabe lässt sich mit einer Kreuztabelle einfacher durchführen.

☛ *Weitere Informationen zu den Anfälligkeiten finden Sie unter "Bestand der Bedrohungen und Anfälligkeiten", Seite 61.*

Um Anfälligkeiten auf IT-Assets zu positionieren, gehen Sie wie folgt vor:

1. Klicken Sie auf **Bibliothek > IT-Assets und Anfälligkeiten > Kreuztabelle > Anfälligkeit nach IT-Asset**.
2. Klicken Sie auf **Neu**.
3. Klicken Sie auf **Zeilen hinzuzufügen**, um Anfälligkeiten hinzuzufügen.

4. Klicken Sie auf **Spalten hinzuzufügen**, um IT-Assets hinzuzufügen.
5. Klicken Sie auf die betroffenen Zellen, um Anfälligkeiten und IT-Assets zu verbinden.

> ☛ *Um auf die Anfälligkeiten der Anwendungen zuzugreifen, siehe "Anfälligkeiten einer Anwendung", Seite 59.*

Risiken identifizieren

Um die für ein IT-Asset bestehenden Risiken abzuleiten, können Sie:

- sich auf die Anfälligkeiten stützen, die in der Eigenschaftsseite des Assets identifiziert wurden.

  > ☛ *Weitere Informationen finden Sie unter "Anfälligkeiten einer Anwendung", Seite 59.*

- sich auf die Anfälligkeiten stützen, die mit Bedrohungen verbunden sind.

  > ☛ *Weitere Informationen finden Sie unter "Alle Bedrohungen", Seite 61.*

Risiken auf IT-Assets positionieren

Wenn die Risiken identifiziert sind, bietet **HOPEX IT Risk Management** zwei Methoden zur Positionierung der Risiken.

Risiken über eine Kreuztabelle positionieren

Um die Risiken auf IT-Assets zu positionieren, können Sie eine spezifische Kreuztabelle verwenden.

Um die Kreuztabelle Risiken x IT-Assets zu verwenden, gehen Sie wie folgt vor:

1. Klicken Sie auf **Bibliothek > Risiken > Kreuztabelle > Risiken nach IT-Asset**.
2. Fügen Sie Folgendes hinzu:
   - Risiken in den Zeilen
   - IT-Assets in den Spalten
3. Klicken Sie auf die betroffenen Zellen, um Anfälligkeiten und IT-Assets zu verbinden.

Risiken einzeln auf jedes Asset positionieren

Die Risiken können auf die IT-Assets direkt positioniert werden:

- Anwendungen
- Technologien

Je nach verwendeter Bewertung können Sie Risiken positionieren auf:

- Anwendungen
- bereitgestellte Anwendungen

Weitere Informationen finden Sie unter "Umfang des Risikos", Seite 67.

☛ *Die Positionierung des Risikos wirkt sich auf den Rahmen der Risikobewertung aus. Es stehen zwei Bewertungsvorlagen zur Verfügung. Siehe "Bewertungsvorlagen der Risiken", Seite 79.*

Risikoszenarios identifizieren

Ggf. können Sie Risikoszenarios definieren und die Beziehungen Ursache/Wirkung unter den Risiken identifizieren.

🕮 *Ein IT-Risikoszenario ist die Beschreibung eines IT Ereignisses, das sich auf die Geschäftstätigkeit eines Unternehmens auswirken kann, sofern es eintritt.*

Risikoszenario erstellen

Um ein Risikoszenario zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie auf **Bibliothek > Risiken > Risikoszenarios**.
2. Klicken Sie auf **Erstellen** und anschließend auf **Weiter**.
3. Verbinden Sie im Abschnitt **Elemente eines Risikoszenarios**:
   - Anwendungen oder
   - Softwaretechnologien

☛ *Im Abschnitt **Risiken** werden nicht die Risiken aufgeführt, die aus der Initialisierung des Diagramms stammen.*

Diagramm über Risikoszenario erstellen

Der IT RM Manager identifiziert die Abhängigkeiten vom Typ Ursache / Folge unter den Risiken im Diagramm über ein Risikoszenario. In diesem Diagramm wird ein Risikonetz erstellt, um die zentralen Risiken zu identifizieren.

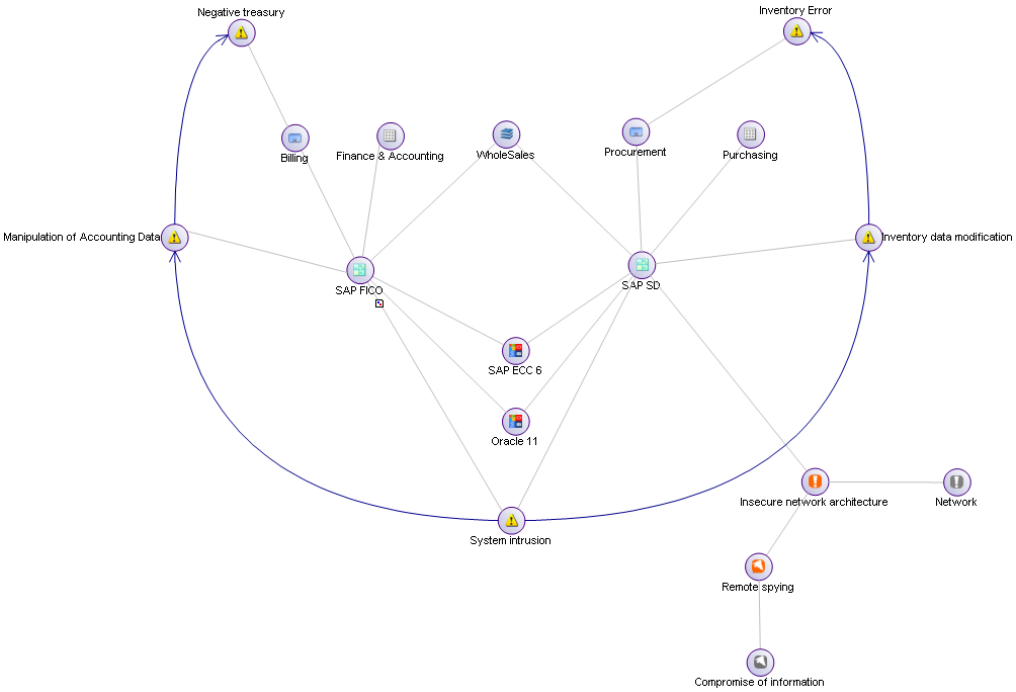
☛ *Weitere Informationen zu den zentralen Risiken finden Sie unter "Zentrale Risiken, Ursachen und Folgen", Seite 75.*

Um ein Diagramm über Risikoszenario zu erstellen, gehen Sie wie folgt vor:

❱ Klicken Sie auf das Symbol des Risikoszenarios und wählen Sie **Neu > Diagramm über Risikoszenario** aus.

Folgende Objekte werden automatisch auf das Diagramm platziert:

- Anwendungen oder Softwaretechnologien
- Anfälligkeiten und Bedrohungen
- Prozesse, Geschäftsfähigkeiten und Geschäftssparten, die mit der Anwendung verbunden sind
- verknüpfte Risiken



Beispiel Diagramm über Risikoszenario

Verbindungen einer Ursache

Die Risiken sind untereinander durch Ursachen verbunden (mit Verbindungen dargestellt). Es handelt sich um szenariospezifische Ursachenverbindungen.

Zentrale Risiken, Ursachen und Folgen

Die Risiken können alternativ betrachtet werden als:

- Ursache
- Folgen
- Zentrales Risiko

Ein zentrales Risiko ist ein Risiko, das in einem Diagramm über ein Risikoszenario mit mindestens einer Ursache und eventuell einer oder mehreren Folgen verbunden ist.

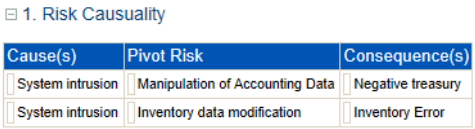
☛ *Ein zentrales Risiko kann mehrere Ursachen und Folgen haben.*

Bericht über die Risikoursache

In einem Bericht können die Verbindungen von Ursachen eines Diagramms über ein Risikoszenario rekapituliert werden.

Um auf den Bericht zuzugreifen, gehen Sie wie folgt vor:

❱ Wählen Sie im Eigenschaftsfenster eines Risikoszenarios die Registerkarte **Bericht über Risikoursache** aus.


1. Risk Causuality

Cause(s)	Pivot Risk	Consequence(s)
System intrusion	Manipulation of Accounting Data	Negative treasury
System intrusion	Inventory data modification	Inventory Error

Beispiel Bericht über Risikoursache

Dieser Bericht hebt die "zentralen Risiken" eines Risikoszenarios hervor, d. h. die Risiken, die sich in der Mitte der Risikokette befinden:

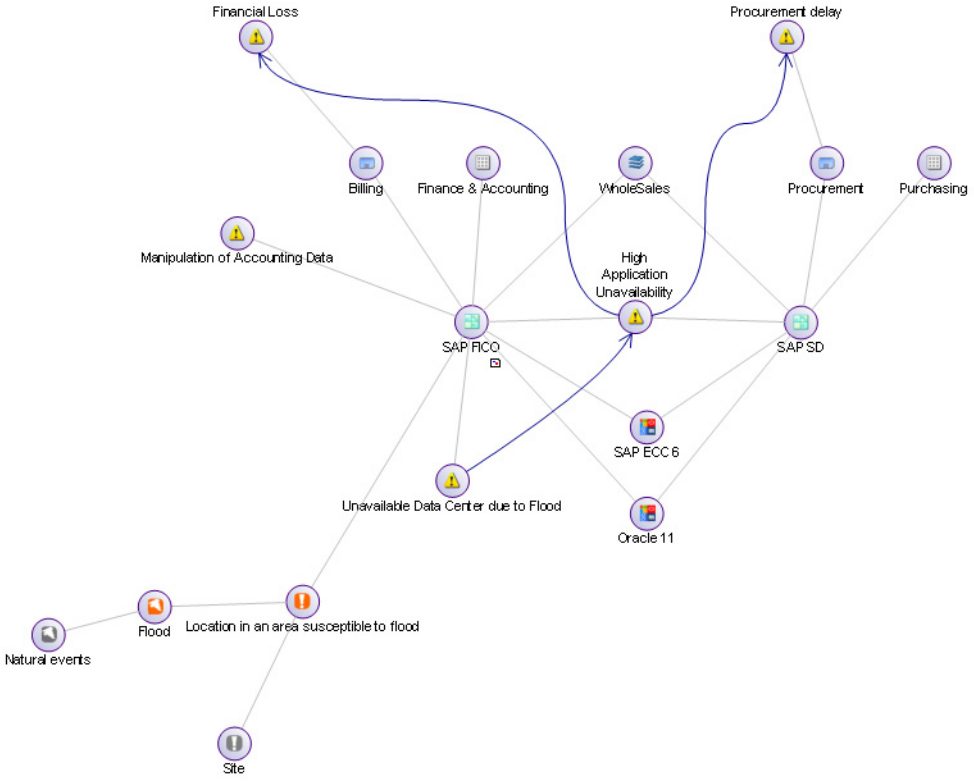
Diese Risikokette enthält:

- Risiken, die als Ursache anscheinend gering sind (beispielsweise IT-Risiken)
- Risiken, die als Folgen potenziell groß sind (beispielsweise große Geschäftsrisiken)

Die Bearbeitung der zentralen Risiken bildet den Schlüssel zur Verhütung dieser großen Risiken.

Beispiele:

Im Folgenden wird ein Diagramm über ein Szenario aufgeführt, das mit einem entsprechenden Ursachenbericht veranschaulicht wird.



Cause	Pivot Risk	Consequence
Unavailable date center due to Flood	High application unavailability	Procurement delay
		Financial Loss

So genannte Experten-Risiken bewerten

HOPEX IT Risk Management ermöglicht, die so genannte Experten-Risikostufe zu bewerten:

- nach Anwendung oder
- nach bereitgestellter Anwendung (um die Risiken einer Entität bewerten zu können)

> ☛ *Die Risiken können entweder auf eine Anwendung oder eine bereitgestellte Anwendung positioniert werden. Ausführliche Informationen finden Sie unter "Umfang des Risikos", Seite 67.*

Direkte Bewertung von Risiken

Die so genannte Experten-Bewertung entspricht der direkten Bewertung in **HOPEX IT Risk Management** (d. h. ohne eine Bewertungskampagne mit Fragebögen).

Risiko nach Anwendung oder Installation

Um ein Risiko direkt zu bewerten, gehen Sie wie folgt vor:

1. Wählen Sie im Eigenschaftsfenster eines Risikos eine der Registerkarten für die Bewertungen aus:
   - Registerkarte **Bewertung nach Installation**: In dieser Registerkarte werden die Risiken pro bereitgestellter Anwendung bewertet
   - Registerkarte **Bewertung nach Anwendung**

   > ☛ *Nur eine dieser Registerkarten wird angezeigt, je nachdem, welche Wahl Sie hinsichtlich der Positionierung der Risiken getroffen haben. Weitere Informationen finden Sie unter "Risiken auf IT-Assets positionieren", Seite 73.*
2. Klicken Sie auf die Schaltfläche **Erweitert**.
3. Wählen Sie eventuell ein Kontextobjekt und anschließend einen Wert aus, für:
   - die Auswirkung

     > 🕮 *Eine Auswirkung beschreibt die Auswirkung des Risikos, wenn das Risiko auftritt.*
   - die Wahrscheinlichkeit

     > 🕮 *Die Wahrscheinlichkeit, dass das Risiko auftritt.*
   - die Geschwindigkeit

     > 🕮 *Die Geschwindigkeit stellt dar, wie schnell sich ein Risiko ab einem Asset bei einem Vorfall auf andere Assets ausweitet.*
4. Ändern Sie eventuell das **Datum der Bemessung** und klicken Sie auf **OK**.

Bewertungsvorlagen der Risiken

Bewertungs-vorlage	Bewertetes Objekt	Kontext	Modus	Bewertete Merkmale	Bewerter
Bewertung der Risiken nach Anwendung	Mit Anwendung verbundenes Risiko	Mit Risiko verbundene Anwendung	direkt oder mit einer Kampagne	- Auswirkung - Wahrscheinlichkeit - Inhärentes Risiko - Geschwindigkeit - Gewichtetes inhärentes Risiko	- Direkte Bewertung: IT RM Manager - Mit Kampagne: Eigentümer einer Anwendung
Bewertung der Risiken nach bereitgestellter Anwendung	Mit bereitgestellter Anwendung verbundenes Risiko	Bereitgestellte Anwendung	direkt oder mit einer Kampagne	- Auswirkung - Wahrscheinlichkeit - Inhärentes Risiko - Geschwindigkeit - Gewichtetes inhärentes Risiko	- Direkte Bewertung: IT RM Manager - Mit Kampagne: Eigentümer einer Anwendung

☛ *Diese Bewertungsvorlagen können auch im Rahmen von Bewertungskampagnen verwendet werden. Weitere Informationen finden Sie unter "Bewertungen mit Fragebögen", Seite 87.*

Aktionspläne für eine Verbesserung beschreiben

IT RM Manager:

- definiert die Aktionspläne für eine bessere IT-Kontrolle als Eigentümer eines Aktionsplans
- weist Aktionen den Anwendungseigentümern zu, die für ihre Umsetzung verantwortlich sind

☛ *Sie können Aktionspläne mit IT-Assets verbinden.*

Weitere Informationen zu den Aktionsplänen finden Sie unter "Risiken identifizieren", Seite 109.

IT-COMPLIANCE VERWALTEN

Im Rahmen der Verwaltung von IT-Risiken werden Kontrollen im Hinblick auf die erforderliche Compliance verwendet.

Sie können:

- Kontrollen der Anwendungen dokumentieren, die im Rahmen von geltenden Regelwerken verwaltet werden (Beispiel: ISO 2700x).
- diese Kontrollen mit vorschriftsmäßigen Anforderungen verbinden.

  ☛ *Weitere Informationen zu den Kontrollen finden Sie unter "Die Kontrollen", Seite 40.*
- Kontrollen von so genannten Experten oder über Bewertungskampagnen bewerten.

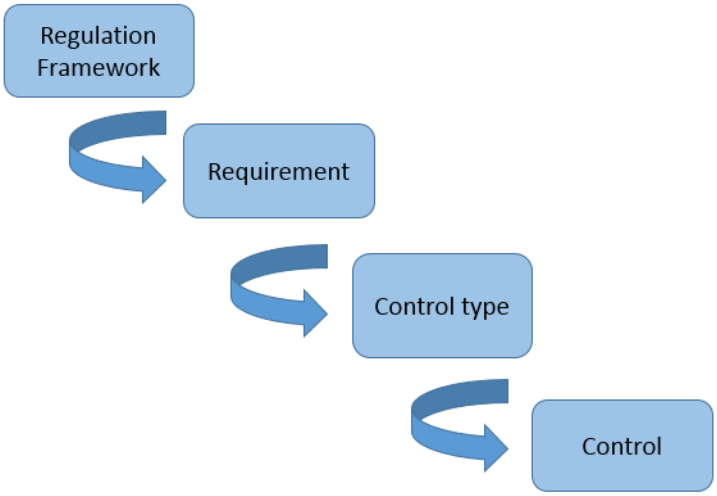
Zu jedem Zeitpunkt können Sie Compliance-Berichte mit einer Synthese hinsichtlich der geltenden Regelwerke und Effizienz des Kontrollsystems generieren.

☛ *Weitere Informationen finden Sie unter "Berichte über IT-Compliance", Seite 135.*

Bestand der Kontrollen und Kontrolltypen aufstellen

Verbindungen zwischen Kontrollen und Kontrolltypen

Wenn Sie eine Kontrolle mit einer Anforderung verbinden wollen, müssen Sie mit der Anforderung den entsprechenden Kontrolltyp verbinden.



Kontrolltypen mit vorschriftsmäßigen Anforderungen verbinden

Um Kontrollen mit vorschriftsmäßigen Anforderungen zu verbinden, gehen Sie wie folgt vor:

1. Wählen Sie im Eigenschaftsfenster einer Anforderung die Registerkarte **Umfang** aus und klappen Sie den Abschnitt **Beitragsleistende Elemente** auf.
2. Verbinden Sie eine oder mehrere Kontrollen.

Umfang der Anwendungen einer Kontrolle

Um die von einer Kontrolle betroffenen Anwendungen zu definieren, gehen Sie wie folgt vor:

1. Wählen Sie im Eigenschaftsfenster einer Anwendung die Registerkarte **Kontrollen** aus und erstellen Sie eine Kontrolle.
2. Klappen Sie im Eigenschaftsfenster der erstellten den Abschnitt **Umfang** auf und verbinden Sie einen **Kontrolltyp**.

Vorschriftsmäßige Anforderungen definieren

Der IT RM Manager definiert die einzuhaltenden vorschriftsmäßigen Anforderungen für die verschiedenen geltenden Regelwerke.

☛ *Diese Vorschriften, Anforderungen oder Kontrolltypen können aus einem UCF- (Unified Compliance Framework®) kompatiblen Bestand importiert werden.*

Um auf die Anforderungen zuzugreifen, gehen Sie wie folgt vor:

❱ Klicken Sie auf **Bibliothek > Vorschriften und Anforderungen**.

☛ *Weitere Informationen zu den Vorschriften und Anforderungen finden Sie unter "Umgebung der Vorschriften", Seite 43.*

Kontrollen der Anwendungen identifizieren

Der IT RM Manager identifiziert bei jeder Anwendung, für die er verantwortlich ist, Folgendes:

- die geltenden Regelwerke oder Anforderungen
- die Kontrollen, auf Grundlage des vordefinierten oder speziell erstellten Kontrollbestands

Um die Kontrollen einer Anwendung zu definieren, gehen Sie wie folgt vor:

1. Wählen Sie im Eigenschaftsfenster der Anwendung die Registerkarte **Kontrollen** aus.
2. erstellen oder verbinden Sie die geltenden Kontrollen.

☛ *Um Bewertungen vorzunehmen müssen die Kontrollen mit den Anwendungen verbunden werden.*

Kontrollen von Experten bewerten

Der IT RM Manager kann Kontrollen direkt bewerten und die Einhaltung (Compliance) der Vorschriften dann ableiten. Hier handelt es sich um die so genannte Expertenbewertung.

Kontrollen direkt bewerten

Um bereitgestellte Kontrollen der Anwendungen direkt zu bewerten, gehen Sie wie folgt vor:

1. Wählen Sie im Eigenschaftsfenster einer Kontrolle die Registerkarte **Bewertung der Kontrollen** aus.
2. Klicken Sie auf die Schaltfläche **Bewerten**.
   Die Liste der von der Kontrolle betroffenen Anwendungen wird angezeigt.
3. Bewerten Sie das **Design** der Kontrolle
   - Adäquat
   - Inadäquat
4. Bewerten Sie die **Effizienz** der Kontrolle.
   - Wirksam
   - Fehlerhaft
5. Ändern Sie eventuell das **Datum der Bemessung** und klicken Sie auf **OK**.

☛ *Das Datum der Bemessung ist standardmäßig das aktuelle Tagesdatum. Sie können ein Datum vor dem aktuellen Tagesdatum auswählen.*

Die **Kontrollstufe** wird automatisch ab den angegebenen Werten der Merkmale berechnet.

Die Kontrollstufe gibt an, inwieweit die bereitgestellten (kontrollierten) Kontrollelemente für die Bewertung eines Risikos effizient sind.

☛ *Die Kontrollstufe wird als "Zufriedenstellend" betrachtet, wenn die Kontrolle wie folgt angezeigt wird:*

- *Wirksam*
- *Adäquat*

Vorlage für die Bewertung der Kontrollen

Bewertungs-vorlage	Bewertetes Objekt	Kontext	Modus	Bewertete Merkmale	Bewerter
Bewertung der Kontrollen nach Anwendung	Kontrolle	Mit Kontrolle verbundene Anwendung	direkt oder mit einer Kampagne	- Design - Effizienz	- IT RM Manager (direkt) - Eigentümer der Kontrollen (Kampagnen)

☛ *Diese Bewertungsvorlage wird auch für die Bewertung von Kontrollen mit Kampagnen verwendet.*

IT-ANBIETER VERWALTEN

HOPEX IT Risk Management ermöglicht, IT-Anbieter zu identifizieren (Softwareunternehmen oder Dienstleister).

Sie können:

- die Kosten der Produkte und Services angeben, die von den einzelnen Anbietern im vorherigen H=Jahr erworben wurden.
- die Anbieter bewerten und ihnen einen Wert zuweisen, indem Sie sich eventuell =auf die über Kampagnen gesendeten Fragebögen stützen.

Zu jedem Zeitpunkt können Sie Berichte mit einer Synthese hinsichtlich der Anbieter-Scores generieren. Weitere Informationen finden Sie unter "Bericht über die Verwaltung der Anbieter", Seite 144.

IT-Anbieter identifizieren

Der funktionale IT RM Administrator identifiziert die IT-Anbieter (Softwareunternehmen, Dienstleister).

☛ *Weitere Informationen zu den Anbietern finden Sie unter "Bestand der Anbieter", Seite 70.*

☛ *Die Anbieter und Technologien können zuvor in **MEGA IT Portfolio Management** oder **MEGA Architecture** identifiziert worden sein.*

Kosten von Produkten und Services angeben

Jedes Jahr erfasst der IT RM Manager ein Element der jährlichen Gesamtkosten von Produkten und Services, die von einem Anbieter erworben wurden.

Auf dieser Grundlage legt er den Rang des Anbieters fest.

☛ *Diese Informationen werden für Dokumentationszwecke in **HOPEX IT Risk Management** eingegeben.*

Um die Kosten einzugeben, gehen Sie wie folgt vor:

1. Klicken Sie auf **Bibliotheken > Anbieter**.
2. Wählen Sie in der angezeigten Liste ein Softwareunternehmen aus.
3. Klicken Sie im Eigenschaftsfenster des Softwareunternehmens auf die Registerkarte **IT-Anbieter**.

4. Geben Sie im Eigenschaftsfenster die Daten im Abschnitt **Finanzinformationen** an:
   - Gesamtbetrag Einkauf
   - Rang

   ☛ *Die Daten in diesem Abschnitt entsprechen den Daten am Jahresende vor dem aktuellen Jahr.*

Sie können zudem folgende Daten eingeben:

- Anschrift
- Informationen der Fakturierung

☛ *Weitere Informationen finden Sie unter "Bestand der Anbieter", Seite 70.*

Anbieter bewerten

Der IT RM Manager kann das mit einem Anbieter verbundene Risiko bewerten.

Um einen Anbieter zu bewerten, gehen Sie wie folgt vor:

1. Klicken Sie auf **Bibliotheken > Anbieter**.
2. Wählen Sie in der angezeigten Liste einen Anbieter aus.
3. Klicken Sie im Eigenschaftsfenster auf die Registerkarte **Bewertung des Anbieterrisikos**.
4. Geben Sie einen Wert ein, der das mit dem Anbieter verbundene Risiko charakterisiert.

   ☛ *Sie können auch Kampagnen starten, um den Anbieter zu bewerten und eventuell Ihre Einschätzung zu bestätigen. In diesem Fall muss der Bewerter in der Bewertungssitzung definiert werden. Weitere Informationen finden Sie unter "Bewertungen mit Fragebögen", Seite 87.*

BEWERTUNGEN MIT FRAGEBÖGEN

MEGA ermöglicht, Bewertungen ab Standardfragebögen durchzuführen. Die Bewertungsfragebögen werden an die entsprechenden Empfänger gesendet.

In diesem Kapitel wird das Prinzip der Bewertungen mit Fragebögen beschrieben. Weitere Informationen zu den verwendeten Bewertungsvorlagen finden Sie im Benutzerhandbuch der von Ihnen verwendeten Lösung.

☛ *Mit den **MEGA**-Lösungen können folgende Bewertungen vorgenommen werden:*

- *von Experten (oftmals direkte Bewertungen genannt)*
- *mit Bewertungskampagnen, in denen Fragebögen gesendet werden, die hier erörtert werden.*

✓ "Prinzip der Bewertung mit Kampagnen", Seite 88
✓ "Bewertungssitzung erstellen", Seite 91
✓ "Bewertungssitzung erstellen", Seite 92
✓ "Sitzungen in einer Kampagne planen (optional)", Seite 94
✓ "Bewertungskampagne freigeben", Seite 97
✓ "zu bewertende Objekte und ihre Kontexte anzeigen", Seite 98
✓ "Umfang der Sitzung und Beantworter definieren", Seite 99
✓ "Zu bewertende Objekte und ihren Kontext freigeben", Seite 100
✓ "Fragebögen senden", Seite 102
✓ "Fragebögen ausfüllen", Seite 103
✓ "Fortschritt der Fragebögen verfolgen", Seite 105
✓ "Bewertungssitzung schließen", Seite 108

PRINZIP DER BEWERTUNG MIT KAMPAGNEN

📖 *Die Bewertung ist ein Mechanismus, mit dem einer identifizierten Population Fragebögen zugesendet werden, um (qualitative oder quantitative) Einschätzungen von identifizierten Objekten zu erhalten. Die Bewertung wird durch Werkzeuge für die Ergebnisanalyse ergänzt.*

Präsentation der Konzepte

Bewertungssitzung

📖 *Eine Bewertungssitzung ist eine Bewertung, die zu einem bestimmten Zeitpunkt gestartet wird. Mit dem Start einer Bewertungssitzung sollen die Fragebögen gezielt an die Benutzer gesendet werden.*

Fragebogen

Die *Fragebögen* einer Bewertung werden an die entsprechenden **Beantworter** gesendet.

📖 *In einem Fragebogen wird eine Liste von vordefinierten Fragen aufgeführt, die für eine Kontrolle gelten können.*

Bewertungskampagne

In den **MEGA**-Lösungen wird eine Bewertungssitzung im Rahmen einer Bewertungskampagne gestartet.

📖 *In einer Kampagne können mehrere Sitzungen gruppiert werden.*

Etappen der Bewertung

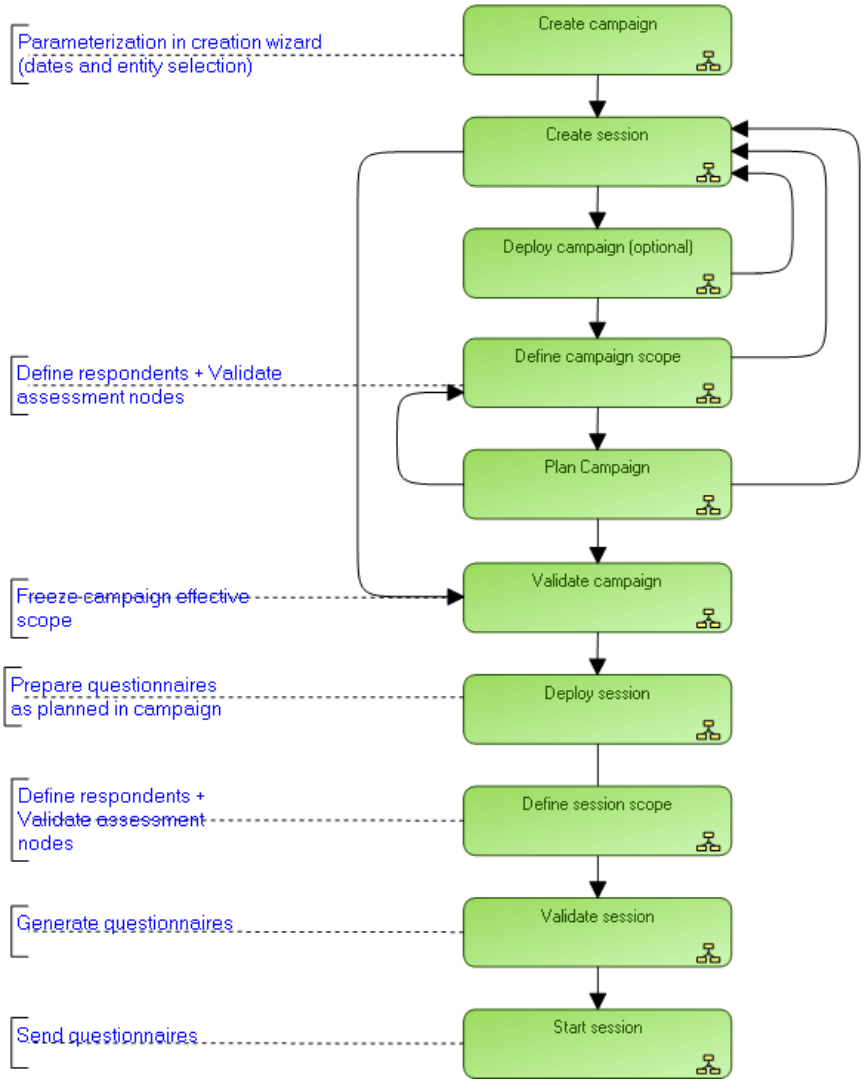
Arbeitsumgebung vorbereiten

Bevor Sie eine Bewertungskampagne starten, müssen Sie die Arbeitsumgebung vorbereiten.

☛ *Weitere Informationen finden Sie unter "Arbeitsumgebung für Fragebögen vorbereiten", Seite 68.*

Kampagne und Bewertungssitzungen starten

Im Folgenden wird ein Beispiel der Etappen aufgeführt die beim Start einer Bewertungskampagne möglich sind:



☛ *Dieses Diagramm ist ein Beispiel für den Ablauf einzelner Etappen einer Bewertungskampagne. Weitere Informationen zu den möglichen Workflows finden Sie unter "Anhang - Workflows", Seite 157*

✓ "Bewertungssitzung erstellen", Seite 91

✓ "Bewertungssitzung erstellen", Seite 92

✓ "Sitzungen in einer Kampagne planen (optional)", Seite 94

☛ *Diese Etappe ist optional. Wenn Sie keine Bewertungskampagne bereitstellen, siehe direkt "Bewertungskampagne freigeben", Seite 97*

✓ "Bewertungskampagne freigeben", Seite 97

✓ "zu bewertende Objekte und ihre Kontexte anzeigen", Seite 98
✓ "Umfang der Sitzung und Beantworter definieren", Seite 99
✓ "Zu bewertende Objekte und ihren Kontext freigeben", Seite 100
✓ "Fragebögen senden", Seite 102

Ordner von Bewertungssitzungen

Nachdem Sie die Bewertungssitzungen gestartet haben, können Sie:

✓ "Fragebögen ausfüllen", Seite 103
✓ "Fortschritt der Fragebögen verfolgen", Seite 105
✓ "Bewertungssitzung schließen", Seite 108

BEWERTUNGSSITZUNG ERSTELLEN

📖 *In einer Kampagne können mehrere Sitzungen gruppiert werden.*

Sie können eine Bewertungskampagne erstellen:

- ***Ab einer Vorlage***
  Mit der Erstellung einer Kampagne mit einer Vorlage können Sie:
  - dieselbe Vorlage bei allen Bewertungssitzungen wiederverwenden
  - den Umfang der Sitzungen definieren und planen, indem Sie die zu bewertenden Elemente innerhalb verschiedener Sitzungen aufteilen
- ***ohne Vorlage***
  Wenn Sie eine Kampagne ohne Vorlage erstellen, können Sie die Vorlage auch angeben, wenn Sie die einzelnen Sitzungen erstellen.

☛ *In dieser Rubrik wird die Erstellung einer Bewertungskampagne mit einer Bewertungsvorlage präsentiert, die standardmäßig mitgeliefert wird. Informationen zu den Möglichkeiten, die von den Bewertungskampagnen geboten werden, finden Sie im Handbuch **MEGA Assessment**.*

Zugriff auf Bewertungskampagnen

Um auf die Bewertungskampagnen zuzugreifen, gehen Sie wie folgt vor:

❱ Klicken Sie auf **Kampagnenmanagement > Kampagnen**.

Bewertungskampagne erstellen

Um eine Bewertungs-*kampagne* zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie **Kampagnenmanagement > Kampagnenmanagement > Kampagnen > Kampagnen > Kampagnen** aus.
   Die Liste der Kampagnen wird im Bearbeitungsbereich angezeigt.
2. Klicken Sie auf **Neu**.
   Daraufhin wird das Fenster zum Erstellen einer Anwendung geöffnet.
3. Wählen Sie im Feld **Kampagnentyp** "mit Vorlage" aus.
4. Wählen Sie die gewünschte **Bewertungsvorlage** aus.
5. Ändern Sie eventuell den **Kalender**.

   ☛ *Im Kalender werden die Anfangs- und die Enddaten der Bewertungskampagne initialisiert.*
6. Geben Sie das **Anfangsdatum** und das **Enddatum** der Bewertung an.
7. Klicken Sie auf **Weiter** und anschließend auf **OK**.
   Die Kampagne wurde erstellt.

Mit den standardmäßig gelieferten Bewertungsvorlagen in der Lösung **HOPEX IT Risk Management** müssen Sie die bei einer Bewertungssitzung zu bewertenden Objekte angeben.

Siehe "Bewertungssitzung erstellen", Seite 92.

BEWERTUNGSSITZUNG ERSTELLEN

Eine Bewertungssitzung ist eine Bewertung, die zu einem bestimmten Zeitpunkt gestartet wird. Mit dem Start einer Bewertungssitzung sollen die Fragebögen gezielt an die Benutzer gesendet werden.

Zugriff auf Bewertungssitzungen

Um auf eine Bewertungssitzung zuzugreifen, gehen Sie wie folgt vor:

1. Klicken Sie auf **Bewertungskampagnen** und wählen Sie die betreffende Bewertungskampagne aus.

   ☛ *Um auf die Kampagne zuzugreifen, siehe "Zugriff auf Bewertungskampagnen", Seite 91.*

2. Wählen Sie im Eigenschaftsfenster der Bewertungskampagne die Registerkarte **Sitzungen** aus.

Bewertungssitzung erstellen

Um ein Bewertungssitzung zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie im Eigenschaftsfenster der Kampagne auf die Registerkarte **Sitzungen**.

   ☛ *Um auf die Kampagne zuzugreifen, siehe "Zugriff auf Bewertungskampagnen", Seite 91.*

2. Klicken Sie im Rahmen **Bewertungssitzungen** auf **Neu**.
3. Wählen Sie im Assistenten die zu bewertenden Objekte mit der Schaltfläche **Verbinden** aus und klicken Sie anschließend auf **OK**
   Eine neue Bewertungssitzung wird erstellt.

   ☛ *Im Rahmen einer Bewertungskampagne mit Vorlage wird standardmäßig das Sitzungsmodell angegeben. Es kann nicht geändert werden. Weitere Informationen zur Erstellung von Bewertungssitzungen ohne Vorlage (erweiterter Ad-hoc-Modus) finden Sie im Handbuch **MEGA Assessment**.*

   ☛ *Mit den erstellten Bewertungssitzungen wird die Bewertungskampagne geplant, d. h. die in ihrem Kontext zu bewertenden Objekte werden auf die verschiedenen Bewertungssitzungen aufgeteilt. Siehe "Bewertungen innerhalb verschiedener Sitzungen aufteilen", Seite 95.*

Vorschau der Parameter der Bewertungssitzung

Wenn die Bewertungssitzung erstellt ist, können Sie die Vorschau der vererbten Parameter der Bewertungskampagne erhalten.

☛ *Um auf eine Bewertungssitzung zuzugreifen, siehe "Zugriff auf Bewertungssitzungen", Seite 92*

Um die Vorschau der Parameter zu öffnen, gehen Sie wie folgt vor:

1. Öffnen Sie das Eigenschaftsfenster der Bewertungssitzung und klicken Sie auf die Registerkarte **Parameter und Vorschau**.
   Die Elemente, die bewertet werden, werden angezeigt.

   Vor allem werden angezeigt:

   - die bewerteten Merkmale (die in der Bewertungsvorlage definiert wurden)

     Das bewertete Merkmal legt fest, was bei einer Bewertung bewertet werden soll. Das Merkmal kann mit einer Metaclass verbunden werden, vor allem mit einem der MetaAttributs. Metaclass Risiko, MetaAttribut: Wahrscheinlichkeit.
   - die bewerteten Objekte
   - die Kontextobjekte

     Ein Kontextobjekt ist ein Objekt, in dessen Rahmen eine Bewertung vorgenommen wird. Zum Beispiel kann im Rahmen einer bereitgestellten Anwendung ein Risiko bewertet werden.
   - die Bewertungsknoten, die den Objekten entsprechen, die in die verschiedenen Kontextobjekte platziert wurden, verbunden mit den Beantwortern.

     Ein Bewertungsknoten ist mit Werten verbunden, die ab den Antworten im Fragebogen des Beantworters für jedes bewertete Merkmal berechnet werden. Er wird entweder zum Zeitpunkt der Bereitstellung der Bewertungssitzung oder zum Zeitpunkt der Aggregation erstellt. Die bei der Bereitstellung erstellten Objekte gehören zur Sitzung und legen fest, welches Objekt von wem und in welchem Kontext bewertet werden soll.

Sie können jetzt die Bewertungskampagne freigeben. Siehe "Bewertungskampagne freigeben", Seite 97.

SITZUNGEN IN EINER KAMPAGNE PLANEN (OPTIONAL)

Diese optionale Etappe ist nützlich, wenn mehrere Bewertungssitzungen erstellt werden,

denn Sie können direkt:

- von der Etappe "Bewertungssitzung erstellen", Seite 92:
- zur Etappe "Bewertungskampagne freigeben", Seite 97 wechseln.

Sie können die Bewertungssitzungen innerhalb der Kampagne planen. In diesem Fall müssen Sie folgenden Unteretappen folgen:

- Bewertungskampagne bereitstellen
- Umfang der Bewertungskampagne definieren
- Bewertungen innnerhalb der verschiedenen Sitzungen aufteilen

Bewertungskampagne bereitstellen

Bei der Bereitstellung einer Bewertungskampagne werden im Voraus die zu bewertenden Objekte bei jeder Sitzung der Kampagne angegeben.

☛ *Diese Etappe ist optional. Wenn Sie keine Bewertungskampagne bereitstellen möchten, siehe direkt "Bewertungskampagne freigeben", Seite 97*

Um eine Kampagne bereitzustellen, gehen Sie wie folgt vor:

1. Klicken Sie in der Liste der Kampagnen auf das Symbol der erstellten Kampagne und wählen Sie **Bewertungskampagne (in Vorbereitung) > Bereitstellen** aus.

   ☛ *Um auf die Kampagne zuzugreifen, siehe "Zugriff auf Bewertungskampagnen", Seite 91.*

2. Geben Sie im Fenster der Bereitstellung an, dass die Kampagne sofort bereitgestellt werden soll.

   ☛ *In einem Fenster werden Sie gefragt, ob die Kampagne bereitgestellt werden soll:*

   - *jetzt ausführen*
   - *sobald wie möglich ausführen (nach Veröffentlichung)*
   - *zum geplanten Datum und zur geplanten Uhrzeit ausführen*

3. Klicken Sie auf **OK**.
   Es wurden Bewertungsknoten erstellt.

   🕮 *Ein Bewertungsknoten besteht aus:*

   - *einem zu bewertenden Objekt*
   - *einem Beantworter (oder einer Zuweisung, d. h. ein Beantworter, der mit einer bestimmten Geschäftsrolle verbunden ist)*
   - *eventuell einem oder mehreren Kontextobjekten (Entitäten und Prozesse)*

Sie können jetzt den Umfang der Bewertungskampagne definieren. Siehe "Umfang der Bewertungskampagne und Beantworter definieren", Seite 95.

Umfang der Bewertungskampagne und Beantworter definieren

Nach der Bereitstellung der Bewertungskampagne müssen Sie:

- den Umfang definieren, d. h. die Bewertungsknoten auswählen, die eingefügt werden sollen.
- Beantworter angeben

> ☛ *Weitere Informationen zu den Bewertungsknoten finden Sie unter "Bewertungskampagne bereitstellen", Seite 94.*

Umfang der Bewertungskampagne definieren

Um den Umfang der Kampagne zu definieren, gehen Sie wie folgt vor:

1. Klicken Sie im Eigenschaftsfenster der Kampagne auf die Registerkarte **Effektiver Umfang**.

   > ☛ *Um auf die Kampagne zuzugreifen, siehe "Zugriff auf Bewertungskampagnen", Seite 91.*

   Die Liste der Bewertungsknoten aus der Bereitstellung wird angezeigt.
2. Wählen Sie die Werte aus, die aus der Kampagne entfernt werden sollen und klicken Sie auf die Schaltfläche **Ungültig machen**.

Beantworter angeben

Um Beantworter hinzuzufügen oder zu ändern, gehen Sie wie folgt vor:

❱ Wählen Sie die betreffenden Elemente aus und klicken Sie auf **Beantworter definieren**.

Bewertungen innerhalb verschiedener Sitzungen aufteilen

Wenn der Umfang der Kampagne definiert wurde und die Bewertungssitzungen erstellt wurden, können Sie die Kampagne planen.

Hier teilen Sie die Bewertungen innerhalb verschiedener Bewertungssitzungen auf.

Um eine Kampagne zu planen, gehen Sie wie folgt vor:

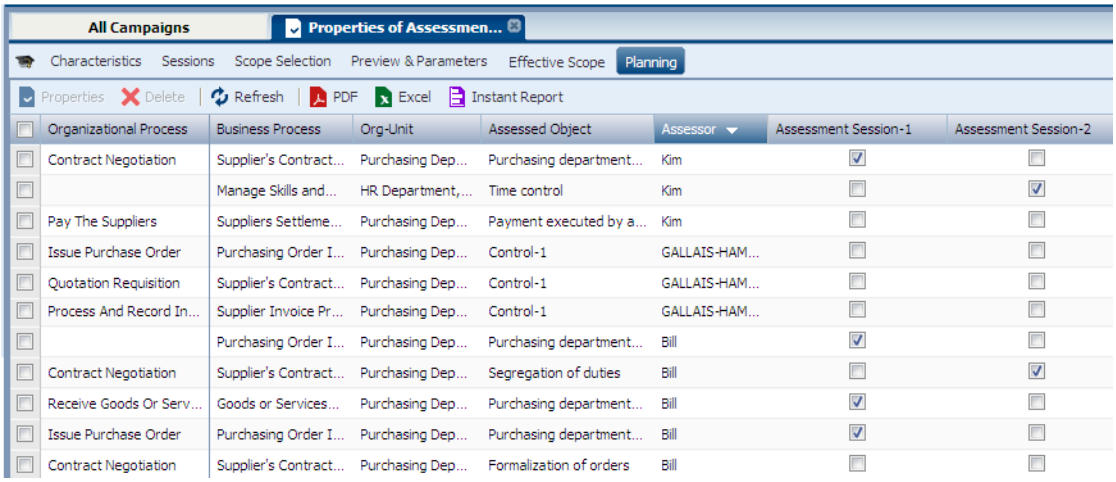
1. Öffnen Sie das Eigenschaftsfenster der Bewertungskampagne klicken Sie auf die Registerkarte **Planung**.

   > ☛ *Um auf die Kampagne zuzugreifen, siehe "Zugriff auf Bewertungskampagnen", Seite 91.*

   Die Registerkarte **Planung** wird nur angezeigt, wenn Bewertungssitzungen erstellt wurden.

2. Wählen Sie im rechten Teil des Fensters die Bewertungssitzungen aus, in denen ein Objekt in seinem Kontext bewertet werden soll.

   ☛ *Wenn die zuvor erstellten Bewertungssitzungen nicht angezeigt werden, klicken auf die Schaltfläche* ***Auffrischen****.*



Organizational Process	Business Process	Org-Unit	Assessed Object	Assessor	Assessment Session-1	Assessment Session-2
Contract Negotiation	Supplier's Contract...	Purchasing Dep...	Purchasing department...	Kim	☑	☐
	Manage Skills and...	HR Department,...	Time control	Kim	☐	☑
Pay The Suppliers	Suppliers Settleme...	Purchasing Dep...	Payment executed by a...	Kim	☐	☐
Issue Purchase Order	Purchasing Order I...	Purchasing Dep...	Control-1	GALLAIS-HAM...	☐	☐
Quotation Requisition	Supplier's Contract...	Purchasing Dep...	Control-1	GALLAIS-HAM...	☐	☐
Process And Record In...	Supplier Invoice Pr...	Purchasing Dep...	Control-1	GALLAIS-HAM...	☐	☐
	Purchasing Order I...	Purchasing Dep...	Purchasing department...	Bill	☑	☐
Contract Negotiation	Supplier's Contract...	Purchasing Dep...	Segregation of duties	Bill	☐	☑
Receive Goods Or Serv...	Goods or Services...	Purchasing Dep...	Purchasing department...	Bill	☑	☐
Issue Purchase Order	Purchasing Order I...	Purchasing Dep...	Purchasing department...	Bill	☑	☐
Contract Negotiation	Supplier's Contract...	Purchasing Dep...	Formalization of orders	Bill	☐	☐

☛ *Die Beantworter werden in der Etappe "Umfang der Bewertungskampagne und Beantworter definieren", Seite 95 angegeben.*

BEWERTUNGSKAMPAGNE FREIGEBEN

Sie können die Bewertungskampagne freigeben:

- direkt nach der Erstellung einer Sitzung oder
- nach der Planung der Kampagne

> ☛ *Weitere Informationen finden Sie unter "Bewertungssitzung erstellen", Seite 92 und "Sitzungen in einer Kampagne planen (optional)", Seite 94.*

Mit der Freigabe der Bewertungskampagne werden ihre Parameter (zum Beispiel Umfang oder Planung) festgelegt.

Um eine Kampagne freizugeben, gehen Sie wie folgt vor:

❱ Klicken Sie auf das Symbol der Kampagne und wählen Sie **Bewertungskampagne (in Vorbereitung) > Freigeben** aus.

> ☛ *Um auf die Kampagne zuzugreifen, siehe "Zugriff auf Bewertungskampagnen", Seite 91.*

Sie können jetzt den Start der Bewertungssitzung vorbereiten und die Bewertungssitzung bereitstellen. Siehe "zu bewertende Objekte und ihre Kontexte anzeigen", Seite 98.

ZU BEWERTENDE OBJEKTE UND IHRE KONTEXTE ANZEIGEN

Nach Freigabe der Kampagne können Sie die zu bewertenden Objekte und ihre Kontexte definieren. Dazu müssen Sie ***die Bewertungssitzung bereitstellen***.

Mit der Bereitstellung werden alle möglichen Bewertungsknoten für die Sitzung berechnet.

> 🕮 *Ein Bewertungsknoten besteht aus:*
>
> - *einem zu bewertenden Objekt*
> - *einem Beantworter (oder einer Zuweisung, d. h. ein Beantworter, der mit einer bestimmten Geschäftsrolle verbunden ist)*
> - *eventuell einem oder mehreren Kontextobjekten (Entitäten und Prozesse)*

Der Verantwortliche der Sitzung kann diese Liste anschließend erhalten.

Um die Liste der Bewertungsknoten einer Sitzung zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie das Eigenschaftsfenster der Kampagne und klicken Sie auf die Registerkarte **Sitzung**.

   > ☛ *Um auf die Kampagne zuzugreifen, siehe "Zugriff auf Bewertungskampagnen", Seite 91.*

2. Klicken Sie im Abschnitt **Bewertungssitzung** auf die betreffende Sitzung und wählen Sie **Bewertungssitzung (einzureichen) > Bereitstellen** aus.

   > ☛ *In einem Zwischenfenster werden Sie gefragt, ob die Bereitstellung jetzt, sobald wie möglich oder zu einem geplanten Datum ausgeführt werden soll.*

   Dieser Vorgang kann einige Minuten in Anspruch nehmen.

UMFANG DER SITZUNG UND BEANTWORTER DEFINIEREN

Nach der Bereitstellung der Bewertungssitzung müssen Sie:

- die Bewertungsknoten auswählen, die in der Sitzung enthalten sein sollen, d. h. den Umfang der Sitzung definieren.
- Beantworter angeben

> ☛ *Wenn Sie den Umfang er Bewertungskampagne definiert haben, müssen Sie nicht zwangsläufig den Umfang bei der Bewertungssitzung neu definieren. Weitere Informationen finden Sie unter "Umfang der Bewertungskampagne und Beantworter definieren", Seite 95.*

Umfang der Sitzung definieren

Um auf die Liste der berechneten Bewertungsknoten zuzugreifen, gehen Sie wie folgt vor:

❱ Öffnen Sie das Eigenschaftsfenster der Bewertungssitzung und klicken Sie auf die Registerkarte **Effektiver Umfang**.

> ☛ *Um auf die Sitzung zuzugreifen, siehe "Zugriff auf Bewertungssitzungen", Seite 92.*

Sie können jetzt die zu bewertenden Objekte in der Sitzung auswählen.

Ab dieser Liste können Sie:

- die zu bewertenden Elemente duplizieren, freigeben, ungültig machen oder löschen
- ihnen einen Beantworter zuweisen.

Beantworter angeben

Um Beantworter hinzuzufügen oder zu ändern, gehen Sie wie folgt vor:

❱ Wählen Sie im Eigenschaftsfenster der Sitzung in der Registerkarte **Effektiver Umfang** die betreffenden Elemente und klicken Sie auf **Beantworter definieren**.

> ☛ *Um auf die Sitzung zuzugreifen, siehe "Zugriff auf Bewertungssitzungen", Seite 92.*

ZU BEWERTENDE OBJEKTE UND IHREN KONTEXT FREIGEBEN

Mit der Freigabe der Bewertungssitzung werden die zu bewertenden Objekte in ihrem Kontext und die Beantworter freigegeben.

Mit dieser Freigabe werden ***Fragebögen generiert***, ohne sie jedoch an die Empfänger zu senden.

Bewertungssitzung freigeben

Um die Sitzung freizugeben und demnach Fragebögen zu generieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Eigenschaftsfenster der Kampagne und klicken Sie auf die Registerkarte **Sitzung**.

   ☛ *Um auf die Kampagne zuzugreifen, siehe "Zugriff auf Bewertungskampagnen", Seite 91.*

2. Klicken Sie im Abschnitt **Bewertungssitzung** auf die betreffende Sitzung und anschließend auf **Bewertungssitzung > Freigeben**.
   Alle Fragebögen werden mit dem Status "zu senden" erstellt. Dieser Vorgang kann einige Minuten in Anspruch nehmen.

Sie können nun die generierten Fragebögen anzeigen.

Generierte Fragebögen anzeigen

Um die generierten Fragebögen anzuzeigen, gehen Sie wie folgt vor:

1. Klicken Sie im Eigenschaftsfenster einer Bewertungssitzung auf die Registerkarte **Fragebögen**.

   ☛ *Um auf die Sitzung zuzugreifen, siehe "Zugriff auf Bewertungssitzungen", Seite 92.*

2. Wählen Sie die entsprechende Linie der Bewertungssitzung aus und klicken Sie auf **Fragebögen anzeigen**.
3. Öffnen Sie die einzelnen Fragebögen, um die Bewertungsknoten und die jeweils verbundenen Fragen anzuzeigen.

   ☛ *Wenn Ihnen die Präsentation der Fragebögen nicht gefällt, können Sie vom funktionalen Administrator an dieser Stelle noch geändert werden. Weitere Informationen finden Sie im Handbuch **MEGA Assessment**, im Kapitel "Bewertungsvorlagen". Die Fragebogenvorlagen sind in dieser Lösung in der Registerkarte für das*

Kampagnenmanagement ***> Vorbereitung > Fragebogenvorlage*** *verfügbar.*

☛ *An dieser Stelle können Sie die Präsentation der Fragebögen noch ändern.*

☛ *Sie sollten die Bewertungssitzung kurz vor dem Start der Sitzung freigeben. Wenn Sie sie zu früh freigeben, können die Informationen über die Beantworter falsch sein.*

Fragebögen neu generieren

Sie müssen Sie Fragebögen eventuell neu generieren, wenn Sie beispielsweise die Beantworter ändern möchten, bevor die Bewertungssitzung gestartet wird.

Um Fragebögen neu zu generieren, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf die betreffende Bewertungssitzung und wählen Sie **Bewertungssitzung (zu starten) > Fragebögen neu generieren** aus.

   ☛ *Um auf die Sitzung zuzugreifen, siehe "Zugriff auf Bewertungssitzungen", Seite 92.*

FRAGEBÖGEN SENDEN

Nach der Freigabe der Bewertungssitzung können Sie ***die Bewertungssitzung starten***, wodurch die Fragebögen an die Beantworter gesendet werden.

Um die Bewertungssitzung zu starten, gehen Sie wie folgt vor:

1. Wählen Sie **Bewertungskampagnen > Kampagne > Kampagnen** aus.
   Die Liste der Kampagnen wird in der Navigationsbaumstruktur angezeigt.
2. Wählen Sie die betreffende Kampagne aus und klicken Sie auf **Eigenschaften**.
   Das Eigenschaftsfenster der Kampagne wird im Bearbeitungsbereich angezeigt.
3. Klicken Sie in der Registerkarte **Sitzungen** auf die betreffende Sitzung und anschließend auf **Bewertungssitzung > Starten**.
   Daraufhin wird die Aktivierungsseite der Sitzung angezeigt.
4. Klicken Sie oben auf der Seite auf die Schaltfläche **Speichern**.
   Die *Bewertungsfragebögen* werden an die Beantworter gesendet, die im Umfang der Bewertungssitzung definiert wurden.

FRAGEBÖGEN AUSFÜLLEN

Die hier beschriebenen Etappen beziehen sich auf die Beantworter der Fragebögen.

> ☛ *Weitere Informationen zu den Schritten der Bearbeitung eines Fragebogens finden Sie im Anhang im Absatz über den Workflow der Fragebögen.*

Zugriff auf Bewertungsfragebögen

Nach dem Start einer Bewertungssitzung erhalten die Empfänger eine Benachrichtigung.

Um die Fragebögen zu beantworten, gehen Sie wie folgt vor:

1. Klicken Sie auf **Home > Mein Desktop > Fragebögen > Meine Bewertungsfragebögen**.
   Die Liste der auszufüllenden Fragebögen wird angezeigt.
2. Wählen Sie den betreffenden Fragebogen aus und klicken Sie auf **Fragebogen anzeigen**.
3. Wählen Sie die Fragen hintereinander aus und beantworten Sie sie im unteren Teil des Fensters.
4. Klicken Sie auf **Speichern**.
5. Schließen Sie das Anzeigefenster des Fragebogens.
6. Klicken Sie in der Liste der Fragebögen auf den Fragebogen und wählen Sie **Bewertungsfragebogen (auszufüllen) > Antworten einreichen**.

> ☛ *Die Fragebögen werden in diesem Menü solange angezeigt, bis die Bewertungssitzung geschlossen wird. Wenn die Bewertungssitzung geschlossen ist, können Sie die Fragebögen in der Registerkarte **Fragebögen** im Eigenschaftsfenster der Sitzung anzeigen.*

Übertragung eines Fragebogens beantragen

Falls Sie versehentlich einen Fragebogen erhalten, können Sie den Verantwortlichen der Sitzung bitten, den Fragebogen an eine andere Person zu übertragen.

Um eine Übertragung zu beantragen, gehen Sie wie folgt vor:

1. Klicken Sie auf **Homepage> Mein Desktop > Fragebögen und Checklisten > Meine Bewertungsfragebögen**.

> ☛ *In bestimmten Lösungen zeigt sich das Menü wie folgt an: Risiko > Homepage > Mein Desktop > Meine Verantwortungsbereiche > Meine Bewertungsfragebögen.*

2. Klicken Sie auf das Symbol des Fragebogens und wählen Sie **Bewertungsfragebogen (auszufüllen) > Anforderung einer Übertragung** aus.
   Der Fragebogen wechselt zum Status "Neu zuzuweisen".
   Ein Verantwortlicher wird per E-Mail benachrichtigt und muss den Fragebogen einer anderen Person neu zuweisen.

   ☛ *Anforderungen einer Übertragung treten nur in Ausnahmefällen auf, wenn die Vorbereitungsarbeiten für die Erstellung einer Ausführungskampagne richtig durchgeführt wurden.*

FORTSCHRITT DER FRAGEBÖGEN VERFOLGEN

Ergebnis der Sitzung aufrufen

Um den Fortschritt einer Bewertungssitzung aufzurufen, gehen Sie wie folgt vor:

- Öffnen Sie das Eigenschaftsfenster der Bewertungssitzung und klicken Sie auf die Registerkarte **Berichte > Folgemaßnahmen**.

  ☛ *Um auf die Sitzung zuzugreifen, siehe "Zugriff auf Bewertungssitzungen", Seite 92.*

Gesendete Fragebögen anzeigen

Um auf die Liste der gesendeten Fragebögen zuzugreifen, gehen Sie wie folgt vor:

- Klicken Sie auf **Kampagnenmanagement > Kampagnen > Folgemaßnahmen> Gesendete Fragebögen**.

Bewertungsfragebögen freigeben

Um auf die Liste der von den Beantwortern ausgefüllten Bewertungsfragebögen zuzugreifen, gehen Sie wie folgt vor:

1. Klicken Sie auf **Kampagnenmanagement > Kampagnen > Folgemaßnahmen> Ausgefüllte Fragebögen**.
   Nun erscheint eine Liste der ausgefüllten Fragebögen.
   Der Workflow-Status ist auf den Status "Freizugeben" gewechselt.
2. Wählen Sie den betreffenden Fragebogen aus und klicken Sie auf die Schaltfläche **Fragebögen anzeigen**.
   Der Inhalt des Fragebogens wird in einer neuen Registerkarte angezeigt. Sie können Deliverables erstellen:
3. Schließen Sie das Anzeigefenster des Fragebogens.
4. Wenn der Fragebogen Ihrer Meinung nach richtig ausgefüllt wurde, klicken Sie auf das Symbol des Fragebogens und wählen Sie **Bewertungsfragebogen (freizugeben) > Freigeben** aus.
   Der Fragebogen wird geschlossen und die Ergebnisse werden automatisch berechnet.

Beantworter auffordern, seine Antworten zu ändern

Wenn Sie mit den Antworten eines Fragebogens nicht einverstanden sind, können Sie den Beantworter auffordern, seine Antworten zu ändern.

Um eine Änderung zu beantragen, gehen Sie wie folgt vor:

1. Klicken Sie auf **Kampagnenmanagement > Kampagnen > Folgemaßnahmen> Ausgefüllte Fragebögen**.
2. Klicken Sie auf das Symbol des Fragebogens und wählen Sie **Bewertungsfragebogen (freizugeben) > Neu zuweisen** aus.

☛ *Der Beantworter kann seine Antworten ändern. Siehe "Fragebögen ausfüllen", Seite 103.*

Fragebogen neu zuweisen

Wenn ein Beantworter eine Übertragung angefordert hat, müssen Sie den Fragebogen neu zuweisen.

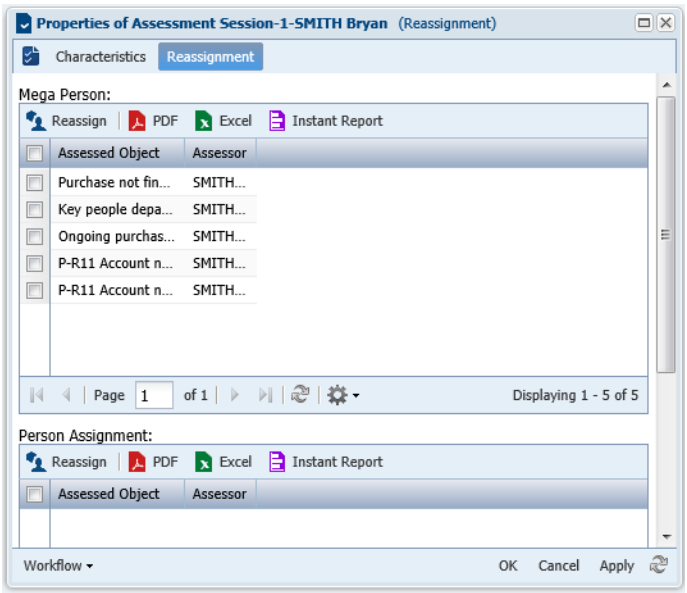
Um einen Fragebogen neu zuzuweisen, gehen Sie wie folgt vor:

1. Wählen Sie in der Liste der gesendeten Fragebögen den betreffenden Fragebogen aus.

   ☛ *Die Fragebögen können über die verschiedenen Menüs abhängig vom verwendeten Desktop aufgerufen werden:*

   - *Bei einer Lösung von **MEGA** können Sie ab der Navigationsregisterkarte **Kampagnenmanagement** auf die Fragebögen zugreifen.*
   - *Im Desktop des Bewertungsmanagers können die Fragebögen ab dem Navigationsfenster **Meine Fragebögen** aufgerufen werden*

2. Öffnen Sie das Eigenschaftsfenster des Fragebogens und klicken Sie auf die Registerkarte **Neuzuweisung**.



☛ *Diese Registerkarte wird nur bei einem Fragebogen mit dem Status "Neu zuzuweisen" angezeigt.*

3. Wählen Sie alle zu bewertenden Knoten und klicken Sie auf die Schaltfläche **Neu zuweisen**.
4. Wählen Sie in dem nun angezeigten Suchfenster die Person aus, die den Fragebogen beantworten muss, und klicken Sie auf **OK**.

   ☛ *Wenn Personenzuweisungen angegeben wurden (zum Beispiel muss der Fragebogen an eine Person im Rahmen einer bestimmten Geschäftsrolle gesendet werden), können Sie den Fragebogen in dem dazu vorgesehenen Abschnitt neu zuweisen.*

   Der neue Beantworter wird in der Spalte **Ansprechpartner** angezeigt.
5. Klicken Sie auf das Symbol des Fragebogens und wählen Sie **Bewertungsfragebogen (neu zuweisen) > Neu zuweisen** aus.

Der neue Beantworter erhält eine E-Mail. Er kann den Fragebogen mit dem Status "In Bearbeitung" ausfüllen und seine Antworten senden.

Bewertungssitzung schließen

Sie können Sie Sitzung jederzeit schließen.

Um eine Bewertungssitzung zu schließen, gehen Sie wie folgt vor:

1. Öffnen Sie das Eigenschaftsfenster der Kampagne und klicken Sie auf die Registerkarte **Sitzung**.

   ☛ *Um auf die Kampagne zuzugreifen, siehe "Zugriff auf Bewertungskampagnen", Seite 91.*

2. Klicken Sie im Abschnitt **Bewertungssitzung** auf das Symbol der betreffenden Sitzung und wählen Sie **Schließen** aus.
   Die Fragebögen werden alle automatisch geschlossen. Dieser Vorgang kann einige Minuten in Anspruch nehmen.

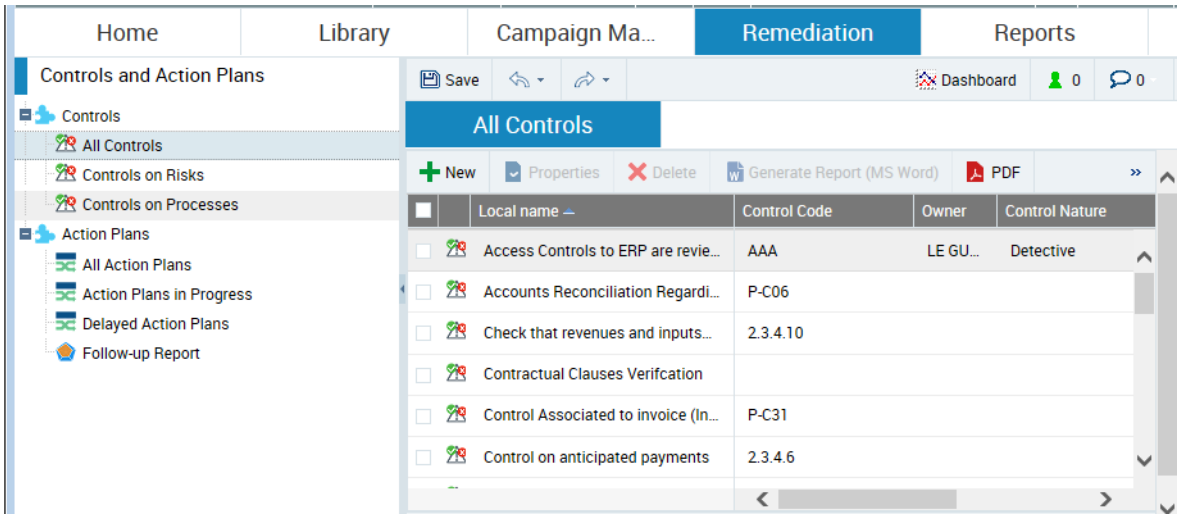
   ☛ *Die Ergebnisse werden nur als gültig betrachtet, wenn die Sitzung geschlossen wurde.*

RISIKEN IDENTIFIZIEREN

Im Rahmen der kontinuierlichen Verbesserung muss ein Unternehmen Maßnahmen ergreifen, um die Ursachen der Nichteinhaltung von IT-Anforderungen zu beseitigen, damit sie sich nicht wieder auftreten.

HOPEX IT Risk Management ermöglicht, festgelegte Aktionspläne anzugeben, umzusetzen und zu verfolgen, um Risiken zu bearbeiten. Die Bearbeitung von Risiken beinhaltet ebenfalls, Kontrollen auszuwählen und durchzuführen, um Risiken zu mindern.

Der IT RM Manager definiert Aktionspläne, mit denen IT-Risiken unter Kontrolle gehalten werden, und weist die Aktionen den Eigentümern der Anwendungen zu, die für diese Aktionen verantwortlich sind.



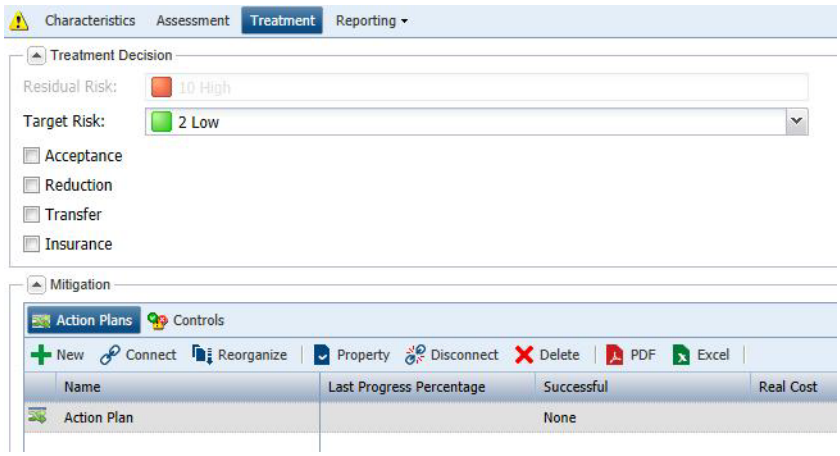
✓ "Modus der Risikobearbeitung", Seite 110
✓ "Aktionspläne verwalten", Seite 113

☛ *Weitere Informationen zu den Aktionsplänen finden Sie im Handbuch **HOPEX Collaboration Manager**.*

MODUS DER RISIKOBEARBEITUNG

Um die Wahl der Bearbeitungen eines Risikos anzugeben, gehen Sie wie folgt vor:

❱ Öffnen Sie das Eigenschaftsfenster des Risikos und klicken Sie auf die Registerkarte **Merkmale**.



☛ *Um auf die Risiken zuzugreifen, siehe "Zugriff auf die Risiken", Seite 66.*

Bearbeitungsmodi

Zum Bearbeiten von Risiken stehen mehrere Lösungen zur Verfügung.

- ***Akzeptanz***
  Die Strategie im Risikomanagement, mit einer fundierten Entscheidung, das Risiko zu akzeptieren. Solange nicht die Absicht gezeigt wird, das Risiko zu bearbeiten, kann die Organisation mit dieser Strategie nicht gegen das Risiko geschützt werden.
- ***Minderung***
  Die Wahrscheinlichkeit des Risikos wird gemindert. Dabei werden weitere Kontrollen eingerichtet oder die Schwere der Folgen reduziert, sollte dieses Risiko auftreten.
- ***Übertragung*** (Zulieferer)
  Das Risiko kann auch mit anderen Partnern geteilt werden, vor allem, wenn die Partner über mehr Kompetenzen verfügen, das Risiko unter Kontrolle zu halten. So kann beispielsweise eine gefährliche Aktivität an einen auf den betreffenden Bereich spezialisierten Partner übertragen werden. In diesem Fall muss oftmals eine neue Untersuchung über die

Risiken durchgeführt werden, da die Einführung eines neuen Partners weitere Risiken mit sich bringen können.

- ***Versicherung***
  Abgesehen von den oben erwähnten Ansätzen muss oftmals eine Versicherung abgeschlossen werden, vor allem für Risiken, die relativ unwahrscheinlich sind, aber eine erhöhte Schwere darstellen. In diesem Fall verlangt die Versicherung im Allgemeinen, Präventionsmaßnahmen zur Risikominderung zu ergreifen.

Die möglichen verschiedenen Szenarios werden analysiert. Dabei werden die positiven und negativen Aspekte verglichen, um ein Szenario zu erhalten, das sich mit der gewünschten Ebene der Risikokontrolle vereinbaren lässt.

Je nach gewählter Lösung müssen ihre Folgen in Bezug auf die Wahrscheinlichkeit und die Auswirkung sowie die Kosten und Nutzen berücksichtigt werden.

Risikostufen

Bei der Wahl einer Lösung muss das Restrisiko unter den von der Geschäftsleitung gewünschten Toleranzwert gebracht werden.

Im Feld **Ziel-Risiko** können Sie die Höhe des Risikos angeben, die von der Organisation akzeptiert wird.

Umzusetzende Kontrollen und Aktionen angeben

Das Management arbeitet mehrere Aktionen aus, um die Höhe der Risiken mit dem Toleranzgrenzwert und dem Risiko-Appetit des Unternehmens abzustimmen.

Bei jedem Risiko wird das gewählte Szenario ausführlich beschrieben. Dabei werden die verschiedenen Risikofaktoren und eingesetzten Kontrollen beschrieben. Zudem wird angegeben, welche Kontrollen eingerichtet werden, um das Risiko zu verhindern, und welche kurativen Abläufe durchgeführt werden, sollte das Risiko auftreten.

Präventive Kontrollen zur Reduzierung der Häufigkeit und der Auswirkung des Risikos können eine Lösung für die Risikominderung sein.

Um die Kontrollen und Aktionspläne für die Risikoverhütung anzugeben, gehen Sie wie folgt vor:

1. Klappen Sie auf der Eigenschaftsseite eines Risikos in der Registerkarte **Bearbeitung** den Abschnitt **Kontrollen und Aktionspläne** auf.
   - In der Registerkarte **Aktionspläne** wird eine Liste der eingerichteten Aktionspläne aufgeführt: zum Beispiel zum Erstellen oder Verbessern einer Kontrolle, für das Krisenmanagement bei einem Zwischenfall

oder für einen vollkommen überarbeiteten Prozess mit dem Ziel, ihn zu verbessern.

> ☛ *Weitere Informationen finden Sie unter "Aktionspläne verwalten", Seite 113.*

- In der Registerkarte **Kontrollen** wird die Liste der Kontrollen aufgeführt, die zur Minderung des Risikos geplant wurden.

  > ☛ *Eine Kontrolle ist ein Mittel, ein oder mehrere Risiken unter Kontrolle zu haben, und sicherzustellen, dass eine gesetzliche, vorschriftsmäßige oder interne Anforderung des Unternehmens erfüllt wird.*

AKTIONSPLÄNE VERWALTEN

Aktionsplan erstellen

Um einen Aktionsplan zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie auf **Bearbeitung > Aktionspläne**.
2. Abschnitt **Aktionspläne**.
3. Klicken Sie auf **Neu**.
   Der Aktionsplan ist nun erstellt.

Sie können die Merkmale des Aktionsplans im Eigenschaftsfenster des Aktionsplans angeben. Siehe "Aktionsplan charakterisieren", Seite 113.

Aktionsplan charakterisieren

Um die Eigenschaften eines Aktionsplans anzugeben, gehen Sie wie folgt vor:

1. Klicken Sie auf **Bearbeitung > Alle Aktionspläne**.
2. Öffnen Sie das Eigenschaftsfenster des betroffenen Aktionsplans.

Allgemeine Merkmale

Sie können folgende Informationen angeben:

- **Name**: Name des Aktionsplans
- **Eigentümer**: Dieses Feld wird standardmäßig von dem Benutzer ausgefüllt, der den Aktionsplan erstellt.
- **Entitätseigentümer**: Entität, die für die Umsetzung eines Aktionsplans verantwortlich ist.
- **Freigabeverantwortlicher**: Benutzer, der für die Freigabe des Aktionsplans verantwortlich ist, wenn alle Aktionen abgeschlossen sind.
- **Mittel**: Text als Beschreibung der notwendigen/gewünschten Mittel für die Ausführung des Aktionsplans.
- **Priorität des Aktionsplans**: um eine Stufe anzugeben. Die Priorität kann verschiedene Stufen haben:
  - "Niedrig"
  - "Mittel"
  - Hoch
  - Kritisch
- **Herkunft**: ermöglicht, den Kontext der Durchführung eines Aktionsplans festzulegen:
  - "Audit"
  - "Konformität"
  - "Ereignis"
  - "Risiko"
  - "RFC"
  - "Sonstiges"
- **Kategorie**: Der Aktionsplan kann beispielsweise verbunden sein mit:
  - Reduzierung der Risikoauswirkung
  - Projektleitung
  - Verbesserung der Prozesse
  - Verbesserung der Kontrollleistung
  - usw.

    ☛ *Zahlreiche weitere Werte sind möglich.*
- **Art**: ermöglicht den Aktionsplan wie folgt zu definieren:
  - Patch
  - Präventiv
- **Kommentare**: ermöglicht, weitere Informationen zum Aktionsplan und zu seinen Merkmalen anzugeben.
- **Lenkungskalender**: ermöglicht, Erinnerungen an die Person zu senden, die für einen Aktionsplan verantwortlich ist, damit sie den Fortschritt angibt, der bei diesem Aktionsplan erzielt wurde.

  ☛ *Standardmäßig wird ein Lenkungskalender zur monatlichen Erinnerung an den Fortschritt mitgeliefert.*

Finanzanalyse

- **Geplante Kosten**: geschätzte Kosten des Aktionsplans.
- **Geplante Kosten (Tag-Mann)**: geschätzte Arbeitslast, die in Tagen/Mann ausgedrückt wird und für die Umsetzung des Aktionsplans notwendig sind.

RACI

Der Benutzer, der für den Aktionsplan als **Durchführungsverantwortlicher** definiert wurde, ist für die Festlegung der durchzuführenden Aktionen und für ihre Durchführung verantwortlich.

Dieses Feld wird von dem Benutzer ausgefüllt, der den Aktionsplan erstellt, oder vom Freigabeverantwortlichen des Aktionsplans.

☛ *Weitere Informationen über die Verwendung von RACI finden Sie unter "Verantwortungsbereiche", Seite 80.*

Erfolgsfaktoren

Im Abschnitt **Schlüsselfaktor für den Erfolg** können Sie Erfolgsindikatoren als Text eingeben, mit denen der Erfolg des Aktionsplans beurteilt werden kann.

Umfang

Um einen Aktionsplan in seiner Umgebung zu positionieren, können Sie im Abschnitt **Umfang** mit dem Aktionsplan Objekte verbinden.

Sie können Objekte folgender Typen verbinden:

- Kontrollen
- Anwendungen
- Risiken
- Entitäten
- Prozesse
- Vorfälle

Meilensteine

Meilensteine sind Schlüsseldaten des Aktionsplans.

☛ *Das geplante Enddatum ist obligatorisch.*

Anlagen

Sie können Geschäftsdokumente als Anlage an einen Aktionsplan anhängen.

☛ *Weitere Informationen zur Verwendung von Geschäftsdokumenten finden Sie im Handbuch **MEGA Common Features**.*

Aktionen verwalten

Der Eigentümer des Aktionsplans muss die Aktionen definieren, mit denen ein Aktionsplan erfolgreich abgeschlossen werden kann. Er kann Aktionen ersten und zuweisen.

🕮 *Eine Aktion ist in einem Aktionsplan enthalten und stellt eine Umwandlung oder eine Bearbeitung in einer Organisation oder einem System dar.*

Um eine Aktion ab einem Aktionsplan zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie auf **Home > Mein Desktop > Meine Verantwortungsbereiche > Meine Aktionspläne**.

   ☛ *Je nach Ihrer Geschäftsrolle können Sie auf Aktionspläne auch über das Menü **Bearbeitung > Mängel und Aktionspläne > Aktionsplan** zugreifen.*
2. Wählen Sie den betreffenden Aktionsplan aus und klicken Sie auf **Eigenschaften**.
3. Klicken Sie im Abschnitt **Aktionen** auf **Neu**.
4. Füllen Sie im Eigenschaftsfenster der Aktion folgende Felder aus:
   - **Priorität**: um eine Stufe anzugeben. Die Priorität kann verschiedene Stufen haben: "niedrig", "mittel", "hoch" oder "kritisch".
   - **Eigentümer**: Verantwortlicher der Aktion wie er vom Ersteller der Aktion bestimmt wurde.
   - **Entitätseigentümer**: Entität, die für die Umsetzung eines Aktionsplans verantwortlich ist.
5. Geben Sie die Meilensteine an, die wichtige Daten der Aktion darstellen.
   - **Geplantes Anfangsdatum**
   - **Geplantes Enddatum**
6. Klicken Sie auf **OK**.
   Die Aktion ist erstellt.

Workflows der Aktionspläne

Je nach Geschäftsrolle der Person, die den Aktionsplan erstellt hat, sind zwei Workflows verfügbar:

- "Top-down"
- "Bottom-up"

☛ *Die Befehle, mit denen auf einen anderen Workflow-Status gewechselt werden kann, werden angezeigt:*

- *im Kontextmenü des Aktionsplans ab einer Liste der Aktionspläne*
- *im Eigenschaftsfenster des Aktionsplans, wenn Sie auf das Symbol des Aktionsplans oben links klicken*

"Bottom-up"-Methode

Bei der "Bottom-up"-Methode wird der Aktionsplan von einem beliebigen Benutzer erstellt (beispielsweise von einem Anwendungseigentümer oder einem IT RM Manager). Der Aktionsplan muss von einem Freigabeverantwortlichen freigegeben werden, damit der Plan umgesetzt werden kann. Genau das ist der Fall, wenn die Beantworter von Fragebögen einen Aktionsplan vorschlagen: Sie müssen ihn zunächst über einen Workflow einreichen.

☛ *Die verschiedenen Etappen des Workflows werden unter "Workflow des Aktionsplans "Bottom-up"", Seite 201*

"Top-down"-Methode

Im Rahmen des Workflows "Top-down " wird der Aktionsplan von einem Verantwortlichen erstellt. In diesem Fall muss der Aktionsplan nicht freigegeben werden.

☛ *Die verschiedenen Etappen des Workflows werden unter "Workflow des Aktionsplans "Top-down"", Seite 202 erklärt.*

Workflow der Aktionen

Wenn die Aktionen eines Aktionsplans definiert sind, werden durch den Start des Aktionsplans die verbundenen Aktionen gestartet.

Sobald der Verantwortliche der Aktion seine Aktionen beendet hat, kann er sie schließen. Mit dem Schließen des Aktionsplans werden die verbundenen Aktionen automatisch geschlossen.

☛ *Siehe "Workflow von Aktionen", Seite 203.*

Folgemaßnahmen bei Aktionsplänen

Fortschritt eines Aktionsplans angeben

Sie können den Fortschrittstatus so erstellen, dass der Fortschritt eines Aktionsplans angeben wird.

Um den Fortschritt eines Aktionsplans anzugeben, gehen Sie wie folgt vor:

1. Klicken Sie auf **Bearbeitung > Aktionspläne**.
2. Wählen Sie einen Aktionsplan aus und öffnen Sie das Eigenschaftsfenster des Aktionsplans.
3. Klappen Sie den Abschnitt **Fortschritt des Aktionsplans** und klicken Sie im Rahmen **Fortschrittstatus** auf **Neu**.
4. Geben Sie einen **Fortschritt in Prozent** an.
5. Geben Sie eventuell eine **Bewertung des Fortschritts** an.
   Sie können beim Aktionsplan Folgendes angeben:
   - Nach Plan
   - In Verzug
6. Klicken Sie auf **OK**.
   Der Fortschrittstatus wurde erstellt. Sie können ihn in regelmäßigen Abständen erstellen.

Berichte über Folgemaßnahmen der Aktionspläne

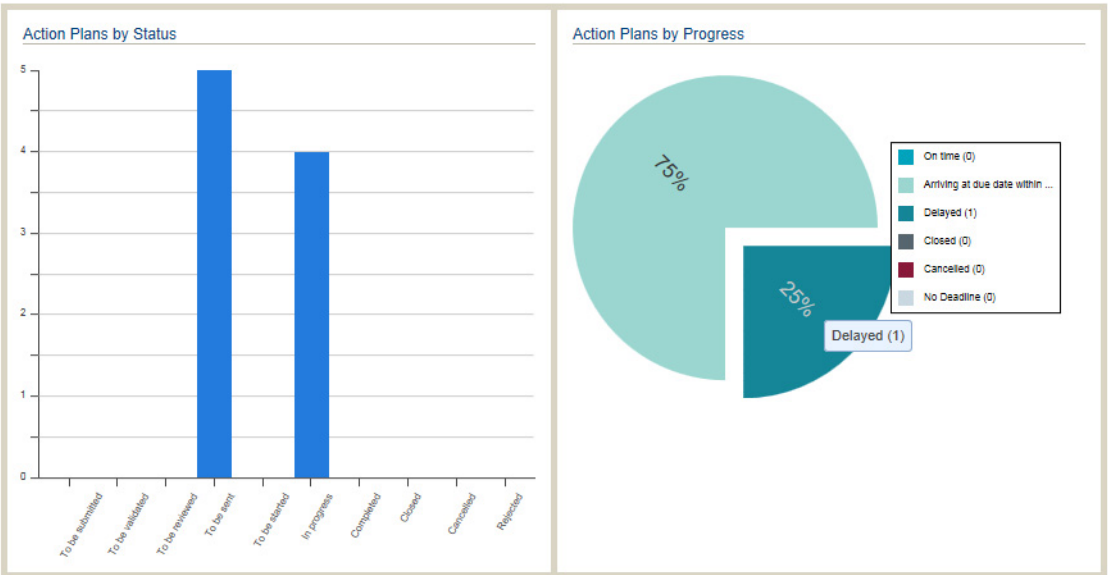
Mit einem Bericht können Sie die Aktionspläne verfolgen.

Für den Zugriff gehen Sie wie folgt vor:

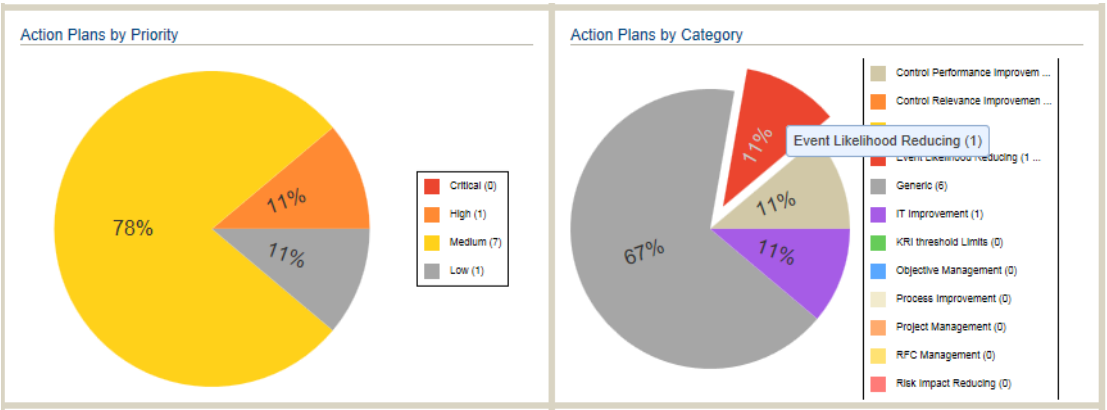
1. Klicken Sie auf **Bearbeitung > Aktionspläne > Bericht über Folgemaßnahmen**.
2. Klicken Sie auf **Erstellen**.*

   ☛ *Sie können in der entsprechenden Registerkarte eventuell Parameter angeben.*

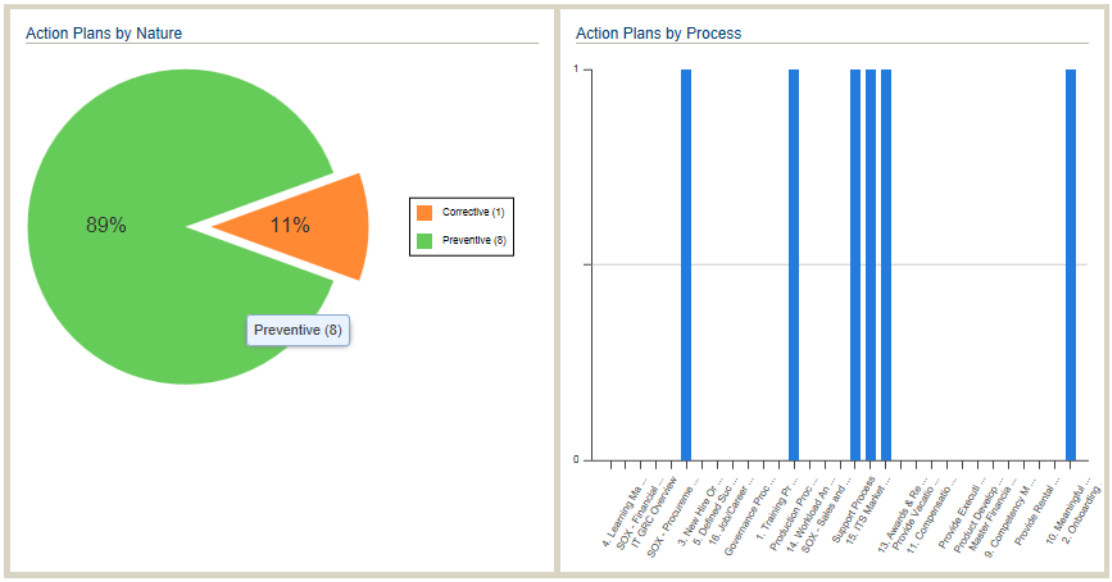
3. Klicken Sie auf die Registerkarte **Berichte**, um das Ergebnis anzuzeigen. Dieser Bericht präsentiert mehrere Balken-/Tortendiagramme, die Aktionspläne darstellen
   - nach Status
   - nach Fortschritt



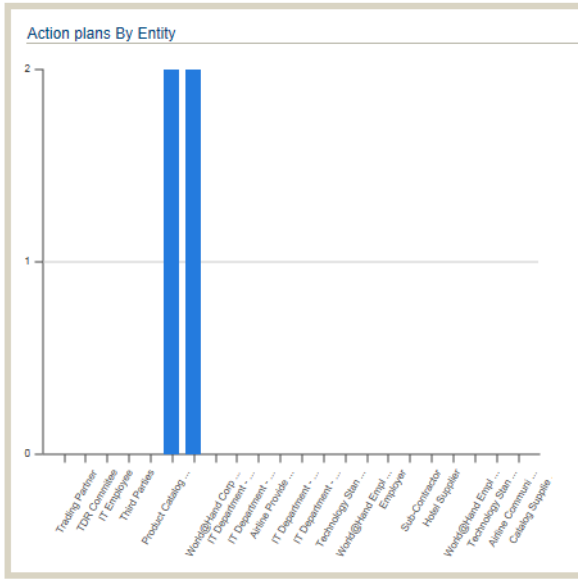
   - nach Priorität
   - nach Kategorie



- nach Art
- nach Prozess



- nach Entität



Um auf die betroffenen Aktionspläne zuzugreifen, gehen Sie wie folgt vor:

1. Klicken Sie auf die Leiste oder den Abschnitt des Diagramms.
2. Die entsprechenden Aktionspläne werden unten auf der Seite in Form einer Liste aufgeführt.

BERICHTE IN HOPEX IT RISK MANAGEMENT

Dieses Kapitel beschreibt die Berichte, die im Rahmen der Lösung **HOPEX IT Risk Management** verwendet werden.

✓ "Zugriff auf Berichte", Seite 122
✓ "Berichte über IT-Risiken", Seite 124
✓ "Berichte über IT-Compliance", Seite 135
✓ "Bericht über die Verwaltung der Anbieter", Seite 144
✓ "Berichte über die Bewertungen", Seite 146
✓ "Berichte über Folgemaßnahmen der Aktionspläne", Seite 163

Die Ergebnisse der Berichte können von der ausgewählten Bewertungsvorlage abhängen.

☛ *Um die Berichte zu personalisieren, siehe Handbuch **MEGA Common Features**, Kapitel "Dokumentation mit MEGA generieren", "Berichte personalisieren".*

Zugriff auf Berichte

Der Zugriff auf die Berichte in **HOPEX IT Risk Management** kann auf verschiedene Weisen erfolgen.

Zugriff auf die Registerkarte der Berichte

In einer eigens hierfür bestimmten Registerkarte werden zahlreiche Berichte aufgeführt.

Für den Zugriff gehen Sie wie folgt vor:

- Klicken Sie im Desktop **HOPEX IT Risk Management** auf die Registerkarte **Berichte**.
  Die Berichte sind nach Themen klassiert:
  - "Berichte über IT-Risiken", Seite 124
  - "Berichte über IT-Compliance", Seite 135
  - "Bericht über die Verwaltung der Anbieter", Seite 144

Zugriff auf Berichte, die direkt bei den Objekten verfügbar sind

Neben den in der Registerkarte aufgeführten Berichten sind Berichte auch verfügbar:

- direkt bei den Objekten
- in verschiedenen Menüs der Lösung, vor allem in Form von Kreuztabellen, mit denen auch das Repository geändert werden kann.

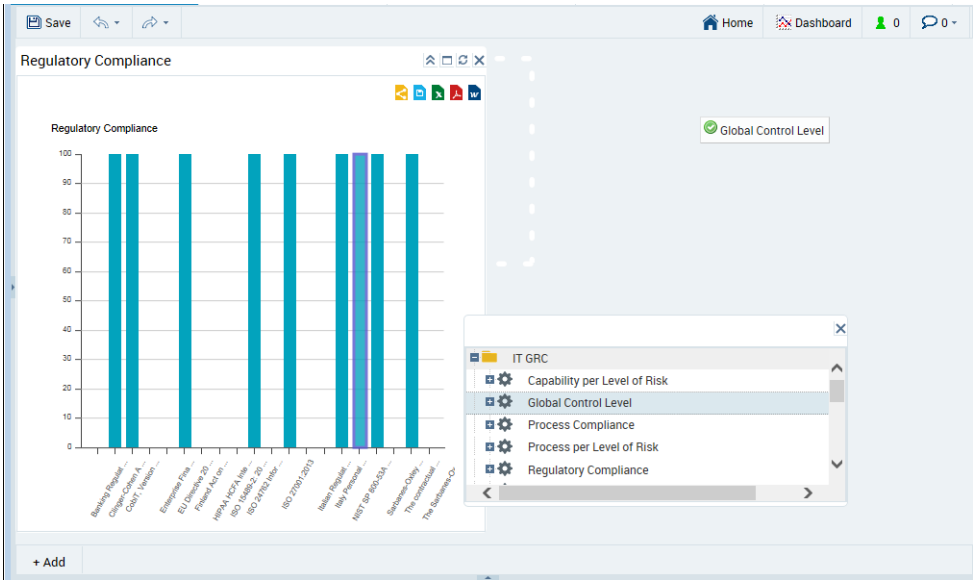
Zugriff auf Widgets

In Ihrem Dashboard können Sie einfach Widgets hinzuzufügen.

Um ein Widget hinzuzufügen, gehen Sie wie folgt vor:

1. Klicken Sie in der Homepage oben rechts auf **Dashboard** und anschließend unten links auf **Hinzufügen**.

2. Wählen Sie in dem nun angezeigten Fenster das Widget aus, das hinzugefügt werden soll, und verschieben Sie es per Drag&Drop auf Ihrem Desktop.



BERICHTE ÜBER IT-RISIKEN

☛ *Weitere Informationen zum Risikomanagement finden Sie unter "IT-Risiken verwalten", Seite 72.*

Berichte über IT-Risiken

Kritizität der Anwendungen

Pfad

Berichte > IT-Risiken > Identifizierung > Kritizität der Anwendungen

Parameter

- Geschäftsprozess: Liste der Geschäftsprozesse

  ☛ *Ein Geschäftsprozess stellt ein System dar, das Produkte oder Dienstleistungen an einen internen oder externen Kunden des Unternehmens oder Organisation liefert. Auf höherer Ebene definiert ein Geschäftsprozess eine Strukturierung und Kategorisierung des Geschäftsbereichs eines Unternehmens. Der Geschäftsprozess kann in weitere Prozesse unterteilt werden. Mit der Verbindung zu den organisatorischen Prozessen kann die reelle Implementierung des Geschäftsprozesses in der Organisation beschrieben werden. Ein Geschäftsprozess kann auch mit einer funktionalen Sicht detailliert werden.*

- Anwendungstyp (optional)

Ergebnis

Dieser Bericht präsentiert in Form von Blasen Anwendungen, die mit Geschäftsprozessen verbunden sind, sowie folgende Angaben:

Auf der Abszisse	Anzahl der Anwendungen mit Schnittstellen zur betroffenen Anwendung über Flüsse
Auf der Ordinate	Anzahl der Geschäftsfähigkeiten, die mit der Anwendung verbunden sind
Blasengröße	Anzahl der Softwareinstallationen der Anwendung
Blasenfarbe	Abhängig von den Gesamtkosten der Anwendung

🕮 *Eine Geschäftsfähigkeit ist eine Einheit zur Aufteilung der Bearbeitungen eines Informationssystems. Bei den Bearbeitungen kann es sich zum Beispiel um die Tätigkeit oder den Geschäftsbereich eines Unternehmens handeln.*

☛ *Diese Gesamtkosten der Anwendung sind in der Lösung **MEGA IT Portfolio Management** verfügbar.*

Beispiel

Tabelle Bedrohungen und Anfälligkeiten

Pfad

Berichte > IT-Risiken > Identifizierung > Tabelle Bedrohungen und Anfälligkeiten

Parameter

- Anfangs- und Enddatum

  ☛ *Mit dem Anfangs- und Enddatum wird der Wertebereich definiert, der für die Bewertungen berücksichtigt wird. Wenn während einer Periode ein Objekt mehrmals bewertet wird, wird die zuletzt durchgeführte Bewertung berücksichtigt.*

- Bedrohungen, die Anfälligkeiten nutzen

  Bedrohungen sind externe oder interne Faktoren, die (IT) Assets des Unternehmens gefährden

  Anfälligkeiten sind Fehler in der Kontrolle eines (IT) Assets, die sie auf eine Bedrohung anfällig machen und zu Mängeln beim Datenschutz, bei der Vollständigkeit oder der Verfügbarkeit dieses Assets führen können.

Ergebnis

Der Bericht präsentiert die Risiken in der Baumstruktur Bedrohung > Anfälligkeit > Anwendung.

Der Bericht zeigt die letzte Beurteilung der Risiken im Kontext der Anwendung an.

Beispiele über Anwendungen

Threat	Vulnerability	Vulnerability Type	IT Asset	Risk	Impact	Inherent Risk	Likelihood	Velocity	Weighted Inherent Risk
Remote spying	Insecure network architecture	Network	SAP FICO	Manipulation of Accounting Data					
Remote spying	Insecure network architecture	Network	SAP FICO	High Application Unavailability	Very High	Very High	Certain	Very High	Very High
Remote spying	Insecure network architecture	Network	SAP FICO	Unavailable Data Center due to Flood					
Remote spying	Insecure network architecture	Network	SAP FICO	System intrusion	Very High	Very High	Certain	Very High	Very High
Remote spying	Insecure network architecture	Network	SAP SD	High Application Unavailability	Very High	Very High	Certain	Very High	Very High
Remote spying	Insecure network architecture	Network	SAP SD	Inventory data modification					
Remote spying	Insecure network architecture	Network	SAP SD	System intrusion	Very Low	Very Low	Rare	Very Low	Very Low

Berichte über IT-Assets

Aggregierte Risikostufe nach Geschäftsprozess

Pfad

Berichte > IT-Risiken > IT-Assets > Aggregierte Risikostufe nach Geschäftsprozess

Parameter

- Anfangs- und Enddatum

  ☛ *Mit dem Anfangs- und Enddatum wird der Wertebereich definiert, der für die Bewertungen berücksichtigt wird. Wenn während einer Periode ein Objekt mehrmals bewertet wird, wird die zuletzt durchgeführte Bewertung berücksichtigt.*

- Bewertungsvorlage:
  - für Anwendungen
  - für Installationen

  ☛ *Weitere Informationen zu den Bewertungsvorlagen finden Sie unter "Bewertungsvorlagen der Risiken", Seite 79.*

- Geschäftsprozess

  ☛ *Ein Geschäftsprozess stellt ein System dar, das Produkte oder Dienstleistungen an einen internen oder externen Kunden des*

Unternehmens oder Organisation liefert. Auf höherer Ebene definiert ein Geschäftsprozess eine Strukturierung und Kategorisierung des Geschäftsbereichs eines Unternehmens. Der Geschäftsprozess kann in weitere Prozesse unterteilt werden. Mit der Verbindung zu den organisatorischen Prozessen kann die reelle Implementierung des Geschäftsprozesses in der Organisation beschrieben werden. Ein Geschäftsprozess kann auch mit einer funktionalen Sicht detailliert werden.

Mit der Schaltfläche **Aggregation generieren** wird die Berechnung gestartet und die Risikobewertungen der Anwendungen und Prozesse konsolidiert.

Ergebnis

Dieser Bericht präsentiert in Form einer Baumstruktur "Geschäftsprozess > Anwendung> Risiken".

Das Ergebnis der Bewertung wird für jedes Element der Baumstruktur angezeigt.

Beispiel

	Impact	Likelihood	Inherent Risk	Velocity	Weighted Inherent Risk
P1	Medium	Likely	Medium	Medium	Medium
A2	High	Likely	High	Medium	High
R1	High	Likely	High	Medium	High
A1	Low	Possible	Medium	Medium	Medium
R3	Medium	Likely	Medium	Medium	Medium
R1	Very Low	Rare	Very Low	Very Low	Very Low
R2	Low	Possible	Low	High	Medium
P2	High	Likely	High	Medium	High
A2	High	Likely	High	Medium	High
R1	High	Likely	High	Medium	High

Heatmaps der Risiken

Pfad

Berichte > IT-Risiken > IT-Assets > Heatmap der Risiken

Parameter

- Anfangs- und Enddatum

  ☛ *Mit dem Anfangs- und Enddatum wird der Wertebereich definiert, der für die Bewertungen berücksichtigt wird. Wenn während einer Periode ein Objekt mehrmals bewertet wird, wird die zuletzt durchgeführte Bewertung berücksichtigt.*

- Risiken: ermöglicht, Risiken auszuwählen und nach verschiedenen Kriterien zu filtern.

Sie können die zu berücksichtigenden Risiken über Baumstrukturen auswählen.

Auswahlkriterium der Risiken	Entsprechende Baumstruktur für die Auswahl
Geschäftssparte	Geschäftssparten > Anwendungen > Risiken
Risikotyp	Risikotypen > Risiken
Prozess	Prozesse > Anwendungen > Risiken
Geschäftsfähigkeit	Geschäftsfähigkeiten > Anwendungen > Risiken
Bedrohungen	Bedrohungen > Anfälligkeiten > Anwendungen > Risiken

Ergebnis

Die Heatmaps veranschaulichen folgende Merkmale:

- Auswirkung / Wahrscheinlichkeit

  📖 *Eine Auswirkung beschreibt die Auswirkung des Risikos, wenn das Risiko auftritt.*

  📖 *Die Wahrscheinlichkeit, dass das Risiko auftritt.*

- Inhärentes Risiko / Geschwindigkeit

  📖 *Ein Bruttorisiko bezeichnet ein Risiko für ein Unternehmen, wenn keine Maßnahmen getroffen werden, die Wahrscheinlichkeit oder Auswirkung dieses Risikos zu ändern. Es handelt sich um den Wert der Auswirkung, der vom Wert der Wahrscheinlichkeit produziert wurde, bevor Präventionsmaßnahmen oder Maßnahmen zur Risikominderung berücksichtigt werden.*

  📖 *Die Geschwindigkeit stellt dar, wie schnell sich ein Risiko ab einem Asset bei einem Vorfall auf andere Assets ausweitet.*

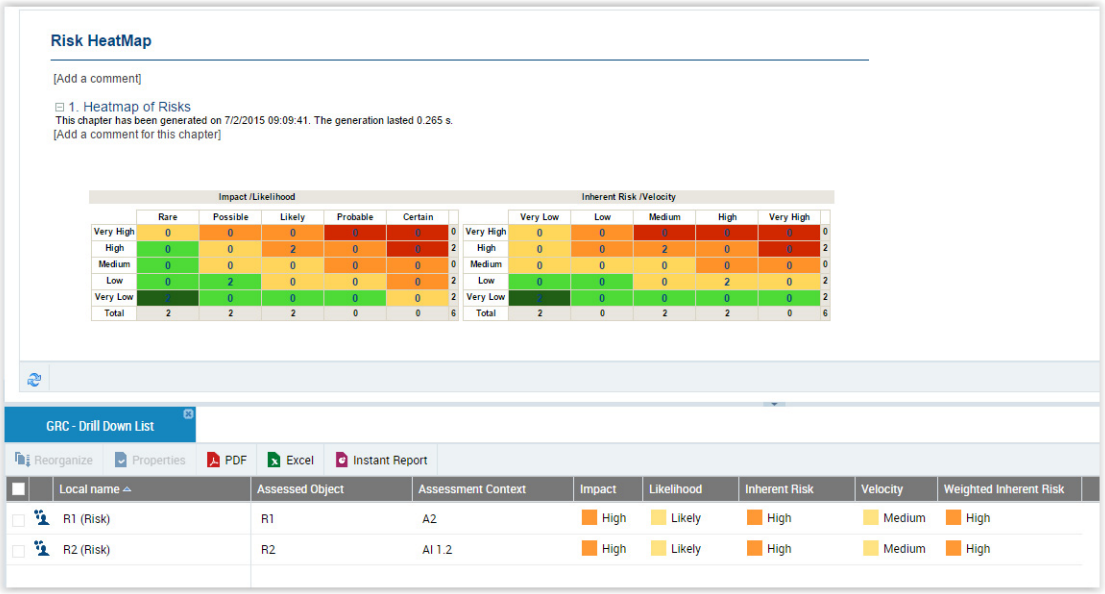
Die Werte der einzelnen Zellen stellen die Bewertungen der ausgewählten Risiken dar.

☛ *Standardmäßig werden alle Risiken berücksichtigt.*

Um die Bewertungen anzuzeigen, die den einzelnen Zellen entsprechen, gehen Sie wie folgt vor:

1. Klicken Sie auf den Wert der Zelle.
   Die Bewertungen werden mit den Angaben des bewerteten Risikos und seines Kontexts (Anwendung oder Softwareinstallation) aufgeführt.

Beispiel


Risk HeatMap
[Add a comment]
1. Heatmap of Risks
This chapter has been generated on 7/2/2015 09:09:41. The generation lasted 0.265 s.
[Add a comment for this chapter]
Impact /Likelihood
Rare Possible Likely Probable Certain
Very High 0 0 0 0 0 0
High 0 0 2 0 0 2
Medium 0 0 0 0 0 0
Low 0 2 0 0 0 2
Very Low 2 0 0 0 0 2
Total 2 2 2 0 0 6
Inherent Risk /Velocity
Very Low Low Medium High Very High
Very High 0 0 0 0 0 0
High 0 0 2 0 0 2
Medium 0 0 0 0 0 0
Low 0 0 0 2 0 2
Very Low 2 0 0 0 0 2
Total 2 0 2 2 0 6
GRC - Drill Down List
Reorganize Properties PDF Excel Instant Report
Local name Assessed Object Assessment Context Impact Likelihood Inherent Risk Velocity Weighted Inherent Risk
R1 (Risk) R1 A2 High Likely High Medium High
R2 (Risk) R2 AI 1.2 High Likely High Medium High

Heatmap der Anwendungen

Pfad

Berichte > IT-Risiken > IT-Assets > Heatmap der Anwendungen

Parameter

- Anfangs- und Enddatum

  ☛ *Mit dem Anfangs- und Enddatum wird der Wertebereich definiert, der für die Bewertungen berücksichtigt wird. Wenn während einer Periode ein Objekt mehrmals bewertet wird, wird die zuletzt durchgeführte Bewertung berücksichtigt.*

- Anwendungen: ermöglicht, die zu berücksichtigenden Anwendungen nach verschiedenen Kriterien und Baumstrukturen auszuwählen.

Auswahlkriterium der Anwendungen	Entsprechende Baumstruktur für die Auswahl
Prozess	Prozess > Anwendungen
Geschäftssparte	Geschäftssparte > Anwendungen
Geschäftsfähigkeit	Geschäftsfähigkeit > Anwendungen

Ergebnis

Die Heatmaps veranschaulichen folgende Merkmale:

- Inhärentes Risiko / Geschwindigkeit

  Ein Bruttorisiko bezeichnet ein Risiko für ein Unternehmen, wenn keine Maßnahmen getroffen werden, die Wahrscheinlichkeit oder Auswirkung dieses Risikos zu ändern. Es handelt sich um den Wert der Auswirkung, der vom Wert der Wahrscheinlichkeit produziert wurde, bevor Präventionsmaßnahmen oder Maßnahmen zur Risikominderung berücksichtigt werden.

  Die Geschwindigkeit stellt dar, wie schnell sich ein Risiko ab einem Asset bei einem Vorfall auf andere Assets ausweitet.

- Auswirkung / Wahrscheinlichkeit

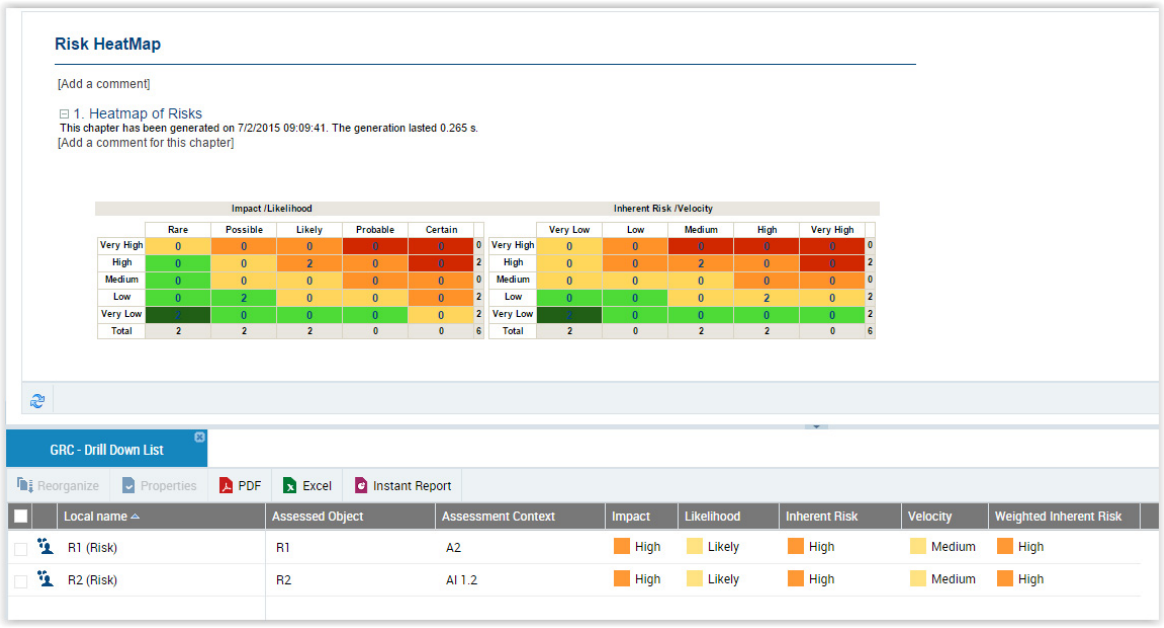
  Eine Auswirkung beschreibt die Auswirkung des Risikos, wenn das Risiko auftritt.

  Die Wahrscheinlichkeit, dass das Risiko auftritt.

Die Werte der einzelnen Zellen stellen die durchschnittliche Risikostufe der Anwendung dar.

Sie können die Bewertungen der Anwendungen anzeigen, wenn Sie auf den Wert der Zelle klicken.

Beispiel



Widgets für Risiken

Um auf die Widgets zuzugreifen, siehe "Zugriff auf Widgets", Seite 122.

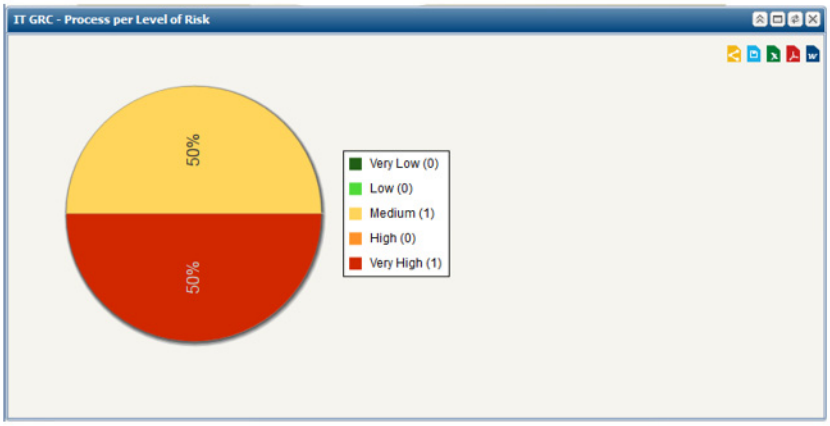
Die Widgets können auf der Homepage im Dashboard aufgerufen werden.

Sie enthaltenen keine Parameter.

Widget Prozesse nach Risikostufe

Mit diesem Widget werden die Geschäftsprozesse der ersten Ebene abhängig vom Wert des durchschnittlichen inhärenten Risikos für den Prozess in Prozenten angezeigt.

> ☛ *Ein Geschäftsprozess stellt ein System dar, das Produkte oder Dienstleistungen an einen internen oder externen Kunden des Unternehmens oder Organisation liefert. Auf höherer Ebene definiert ein Geschäftsprozess eine Strukturierung und Kategorisierung des Geschäftsbereichs eines Unternehmens. Der Geschäftsprozess kann in weitere Prozesse unterteilt werden. Mit der Verbindung zu den organisatorischen Prozessen kann die reelle Implementierung des Geschäftsprozesses in der Organisation beschrieben werden. Ein Geschäftsprozess kann auch mit einer funktionalen Sicht detailliert werden.*
>
> 🕮 *Ein Bruttorisiko bezeichnet ein Risiko für ein Unternehmen, wenn keine Maßnahmen getroffen werden, die Wahrscheinlichkeit oder Auswirkung dieses Risikos zu ändern. Es handelt sich um den Wert der Auswirkung, der vom Wert der Wahrscheinlichkeit produziert wurde, bevor Präventionsmaßnahmen oder Maßnahmen zur Risikominderung berücksichtigt werden.*

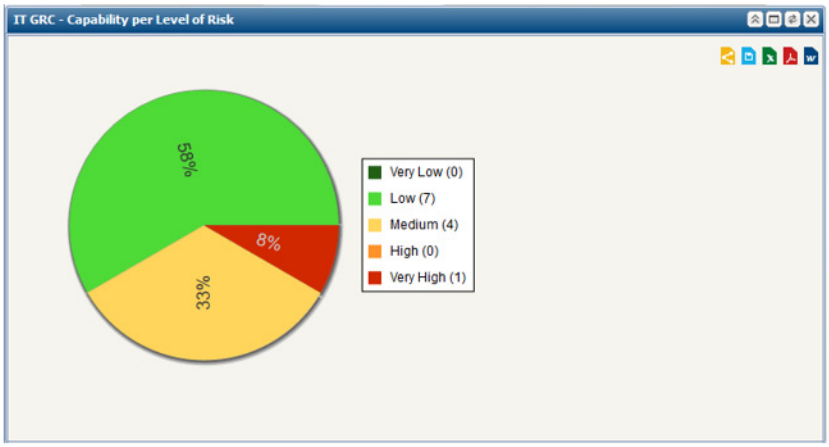


Sie können die entsprechenden Prozesse anzeigen, wenn Sie auf den für Sie interessanten Bereich klicken.

Widget Fähigkeiten nach Risikostufe

Kreisdiagramme mit der Gesamtanzahl der Fähigkeiten in Prozenten auf erster Ebene nach Risikostufe.

> ☛ *Eine Geschäftsfähigkeit ist eine Einheit zur Aufteilung der Bearbeitungen eines Informationssystems. Bei den Bearbeitungen kann es sich zum Beispiel um die Tätigkeit oder den Geschäftsbereich eines Unternehmens handeln.*



Bericht über die Risikoursache

Siehe "Bericht über die Risikoursache", Seite 76.

Berichte über die Anfälligkeiten

Standardmäßig werden Widgets für die Anfälligkeiten mitgeliefert.

☛ *Um auf die Widgets zuzugreifen, siehe "Zugriff auf Widgets", Seite 122.*

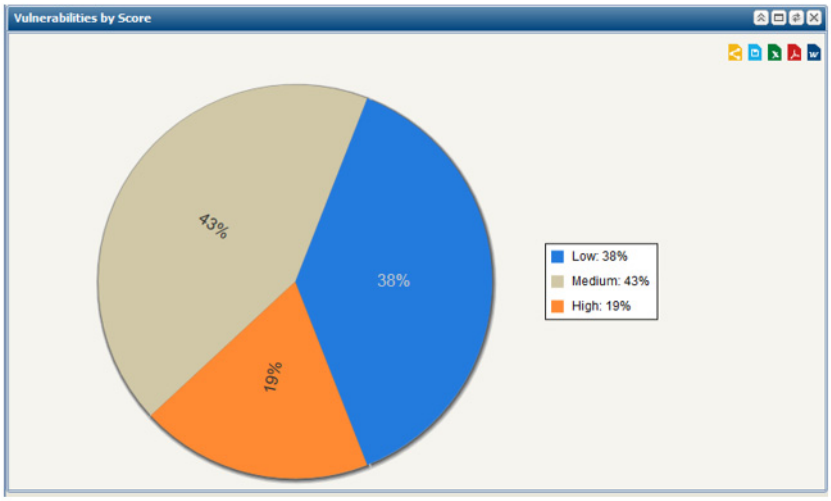
Widget Anfälligkeit nach Score

Kreisdiagramm mit der Anzahl der Anfälligkeiten nach Score:

- Unten
- Mittel
- Oben

🕮 *Anfälligkeiten sind Fehler in der Kontrolle eines (IT) Assets, die sie auf eine Bedrohung anfällig machen und zu Mängeln beim Datenschutz,*

bei der Vollständigkeit oder der Verfügbarkeit dieses Assets führen können.



Sie können die entsprechenden Anfälligkeiten anzeigen, wenn Sie auf den für Sie interessanten Bereich klicken.

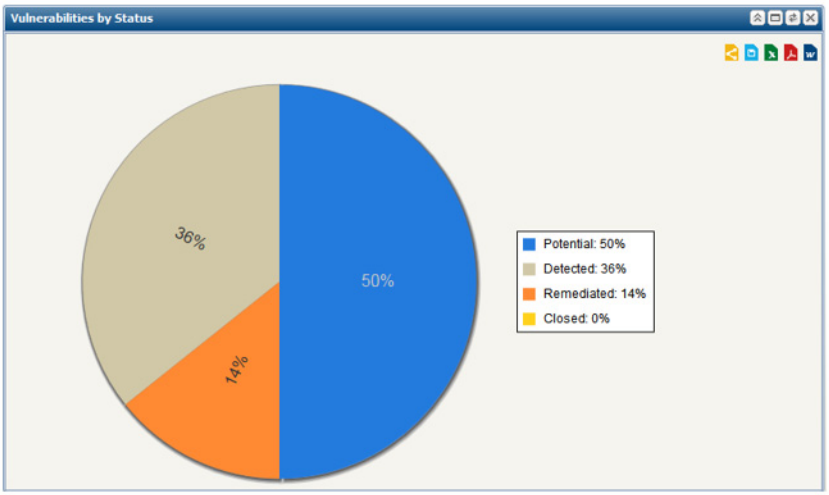
Widget Anfälligkeit nach Status

Kreisdiagramm mit der Anzahl der Anfälligkeiten nach Status:

- Potenzial
- Ermittelt
- Bearbeitet
- Geschlossen

Anfälligkeiten sind Fehler in der Kontrolle eines (IT) Assets, die sie auf eine Bedrohung anfällig machen und zu Mängeln beim Datenschutz,

bei der Vollständigkeit oder der Verfügbarkeit dieses Assets führen können.



Sie können die entsprechenden Anfälligkeiten anzeigen, wenn Sie auf den für Sie interessanten Bereich klicken.

BERICHTE ÜBER IT-COMPLIANCE

☛ *Weitere Informationen finden Sie unter "IT-Compliance verwalten", Seite 80.*

Identifizierung der Kontrollen

Dieser Bericht präsentiert die Aufteilung der Kontrollen nach mehreren Achsen:

- nach Prozess

  ☛ *Ein Geschäftsprozess stellt ein System dar, das Produkte oder Dienstleistungen an einen internen oder externen Kunden des Unternehmens oder Organisation liefert. Auf höherer Ebene definiert ein Geschäftsprozess eine Strukturierung und Kategorisierung des Geschäftsbereichs eines Unternehmens. Der Geschäftsprozess kann in weitere Prozesse unterteilt werden. Mit der Verbindung zu den organisatorischen Prozessen kann die reelle Implementierung des Geschäftsprozesses in der Organisation beschrieben werden. Ein Geschäftsprozess kann auch mit einer funktionalen Sicht detailliert werden.*

- nach Kontrolltyp

  🕮 *Mit einem Kontrolltyp lassen sich die Kontrollen klassieren, die im Unternehmen entsprechend des Standards bzw. Normen der betreffenden Sektoren oder Vorschriften/Reglementierungen (Cobit usw.) implementiert sind.*

- nach Entität

  🕮 *Eine Entität kann eine unternehmensinterne oder -externe Entität sein: Eine interne Entität stellt ein Element der Organisation eines Unternehmens dar, wie beispielsweise eine Direktion, eine Abteilung oder einen Arbeitsplatz. Sie wird auf einer mehr oder weniger genauen Ebene definiert, je nachdem, wie präzise die Angaben über die Organisation sein müssen (siehe Organisationseinheitstyp). Beispiel: Finanzdirektion, Vertrieb, Marketingabteilung, Vertriebsmitarbeiter. Eine externe Organisationseinheit stellt eine Einrichtung dar, die Flüsse mit dem Unternehmen austauscht. Beispiel: Kunde, Lieferant, Administration.*

- nach Ziel

  🕮 *Ein Ziel ist ein Ergebnis, das erreicht werden soll, oder das angestrebte Resultat eines Prozesses oder eines Arbeitsschritts. Mit einem Ziel können die Punkte hervorgehoben werden, die für diesen Prozess oder diesen Arbeitsschritt verbessert werden sollen.*

- nach Regelwerk

  🕮 *Eine Vorschrift oder ein Regelwerk stellt mehrere Richtlinien mit oder ohne Bedingungen auf, die von der Regierung im Rahmen eines Gesetzes, von einem Berufsverband in Form von Best Practices oder intern von einer Organisation festgelegt werden.*

Pfad

Berichte > IT-Compliance > Identifizierung der Kontrollen

Parameter

Hier werden die präsentierten Kontrollen ausgewählt, indem die Elemente angegeben werden, die den Umfang der Kontrollen definieren.

- Kontrolltypen
- Entitäten
- Prozesse
- Ziele

Parameter	Parametertyp	Einschränkungen
Anfangsdatum	Datum	Auswahlkriterium der Bewertungen. Nicht obligatorisch
Enddatum	Datum	Auswahlkriterium der Bewertungen, auf aktuelles Datum festgelegt.
Kontrolltyp des Umfangs	Kontrolltyp	Auswahlkriterium der Kontrollen. Nicht obligatorisch
Entitäten des Umfangs	Entität	Auswahlkriterium der Kontrollen. Nicht obligatorisch
Prozess des Umfangs	Prozesse	Auswahlkriterium der Kontrollen. Nicht obligatorisch
Ziele des Umfangs	Ziel	Auswahlkriterium der Kontrollen. Nicht obligatorisch

Ergebnis

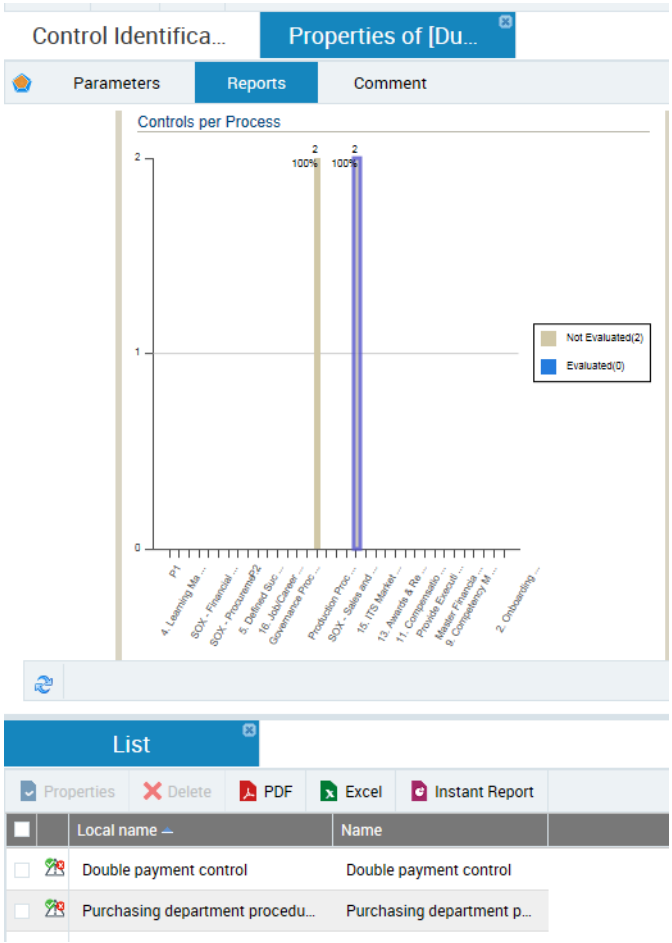
Der Bericht präsentiert die Aufteilung der Kontrollen in Form eines gestapelten Diagramms. Folgende Aufteilungskriterien werden vorgeschlagen:

- Aufteilung nach Prozess
- Aufteilung nach Kontrolltyp
- Aufteilung nach Entität
- Aufteilung nach Entität
- Aufteilung nach Status
- Aufteilung nach Regelwerk

Beispiel

In der folgenden Grafik wird die Anzahl der (bewerteten oder nicht bewerteten) Kontrollen nach Regelwerk aufgeführt.

Wenn Sie auf einen Balken der Grafik klicken, werden die betroffenen Kontrollen in einer Liste unten auf der Seite aufgeführt.



Kontrollstufe nach Vorschrift

Die Kontrollstufe gibt an, inwieweit die bereitgestellten (kontrollierten) Kontrollelemente für die Bewertung eines Risikos effizient sind.

Pfad

Berichte > IT-Compliance > Kontrollstufe nach Vorschrift

Parameter

- Enddatum: standardmäßig das Tagesdatum
- Anfangsdatum: Datum, das dem Enddatum entspricht, aber im vorherigen Jahr
- Vorschriften: alle Vorschriften, mit denen die Kontrollen gefiltert werden (obligatorisch)

  Eine Vorschrift oder ein Regelwerk stellt mehrere Richtlinien mit oder ohne Bedingungen auf, die von der Regierung im Rahmen eines Gesetzes, von einem Berufsverband in Form von Best Practices oder intern von einer Organisation festgelegt werden.

- Prozesse (optional)

  Ein Geschäftsprozess stellt ein System dar, das Produkte oder Dienstleistungen an einen internen oder externen Kunden des Unternehmens oder Organisation liefert. Auf höherer Ebene definiert ein Geschäftsprozess eine Strukturierung und Kategorisierung des Geschäftsbereichs eines Unternehmens. Der Geschäftsprozess kann in weitere Prozesse unterteilt werden. Mit der Verbindung zu den organisatorischen Prozessen kann die reelle Implementierung des Geschäftsprozesses in der Organisation beschrieben werden. Ein Geschäftsprozess kann auch mit einer funktionalen Sicht detailliert werden.

Mit der Schaltfläche **Aggregation generieren** kann die Berechnung gestartet werden.

Ergebnis

Dieser Bericht wird in Form einer Baumstruktur präsentiert, in der die Bewertung jedes einzelnen Elements des Zweigs angezeigt wird. Der Zweig stellt sich wie folgt dar:

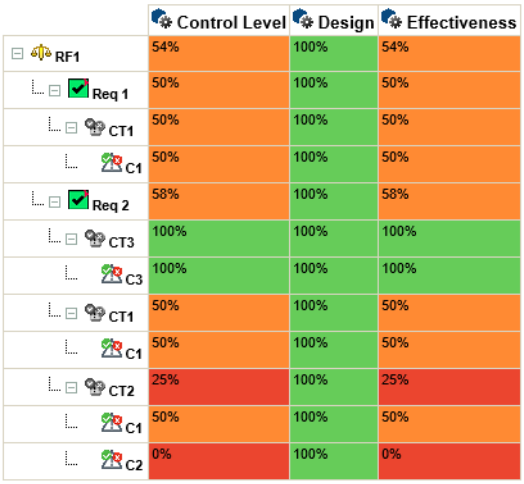
```
Regelwerk > Anforderungen > Kontrolltypen > Kontrollen
```

Bedeutung der Zeilen:

Zeile	Anzeige
Kontrollen	Durchschnitt der Bewertung der Kontrolle (%) für alle verbundenen Anwendungen.
Kontrolltypen	Durchschnitt der Bewertung für Kontrollen des Kontrolltyps

☛ *Eine Kontrolle, die verschiedenen Typen angehört, wird mehrmals "gezählt".*

Beispiel



	Control Level	Design	Effectiveness
RF1	54%	100%	54%
Req 1	50%	100%	50%
CT1	50%	100%	50%
C1	50%	100%	50%
Req 2	58%	100%	58%
CT3	100%	100%	100%
C3	100%	100%	100%
CT1	50%	100%	50%
C1	50%	100%	50%
CT2	25%	100%	25%
C1	50%	100%	50%
C2	0%	100%	0%

Kontrollstufe nach Geschäftsprozess

Die Kontrollstufe gibt an, inwieweit die bereitgestellten (kontrollierten) Kontrollelemente für die Bewertung eines Risikos effizient sind.

Pfad

Berichte > IT-Compliance > Kontrollstufe nach Geschäftsprozess

Parameter

- Enddatum: standardmäßig das Tagesdatum
- Anfangsdatum: Datum, das dem Enddatum entspricht, aber im vorherigen Jahr
- Prozesse (obligatorisch)
- Vorschriften: Ermöglicht, die zu berücksichtigenden Kontrollen zu filtern (optional)

Mit der Schaltfläche **Aggregation generieren** kann die Berechnung gestartet werden.

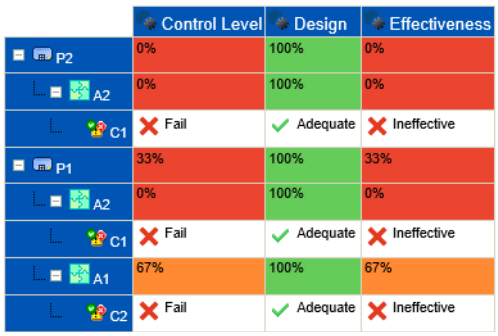
Ergebnis

Dieser Bericht wird in Form einer Baumstruktur präsentiert, in der der Durchschnitt der letzten Bewertung für die einzelnen Elemente der Baumstruktur angezeigt wird.

Die Baumstruktur stellt sich wie folgt dar: Geschäftsprozess > Anwendungen > Kontrollen.

Die Zeile, die sich auf die Kontrolle bezieht, gibt die letzte grundlegende Bewertung der Kontrolle im Kontext der Anwendung an.

Beispiel



	Control Level	Design	Effectiveness
P2	0%	100%	0%
A2	0%	100%	0%
C1	Fail	Adequate	Ineffective
P1	33%	100%	33%
A2	0%	100%	0%
C1	Fail	Adequate	Ineffective
A1	67%	100%	67%
C2	Fail	Adequate	Ineffective

Widgets für Compliance

Die Widgets können auf der Homepage im Dashboard aufgerufen werden.

Sie enthaltenen keine Parameter.

☛ *Um auf die Widgets zuzugreifen, siehe "Zugriff auf Widgets", Seite 122.*

Compliance der Prozesse

Balkendiagramme, die die durchschnittliche Kontrollstufe der Stammprozesse präsentieren.

> 🕮 *Die Kontrollstufe gibt an, inwieweit die bereitgestellten (kontrollierten) Kontrollelemente für die Bewertung eines Risikos effizient sind.*

Um auf die Anwendungen des Prozesses zuzugreifen, gehen Sie wie folgt vor:

1. Klicken Sie auf den entsprechenden Balken.
   Sie erhalten die Liste der Anwendungen des Prozesses mit der durchschnittlichen Compliance-Rate.

Regulatorische Compliance

Balkendiagramm mit:

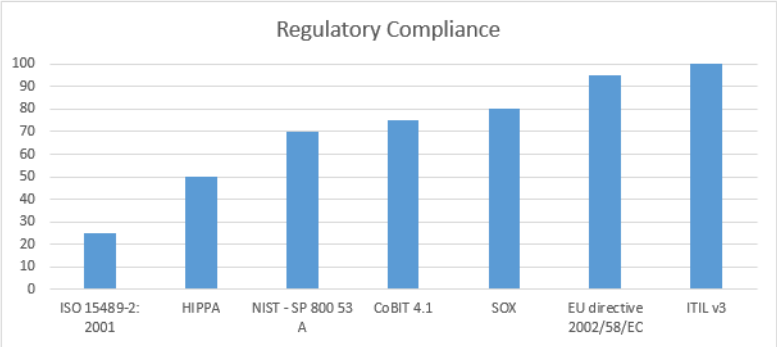
- in der Abszisse: die Stammregelwerke

  > 🕮 *Eine Vorschrift oder ein Regelwerk stellt mehrere Richtlinien mit oder ohne Bedingungen auf, die von der Regierung im Rahmen eines*

Gesetzes, von einem Berufsverband in Form von Best Practices oder intern von einer Organisation festgelegt werden.

- in der Ordinate: die durchschnittliche Kontrollstufe

  📖 *Die Kontrollstufe gibt an, inwieweit die bereitgestellten (kontrollierten) Kontrollelemente für die Bewertung eines Risikos effizient sind.*



Um auf die Anforderungen des Regelwerks zuzugreifen, gehen Sie wie folgt vor:

❱ Klicken Sie auf den entsprechenden Balken.

☛ *Eventuelle Unterregelwerke werden nicht angezeigt.*

Sie erhalten die Liste der Anforderungen des Regelwerks mit der durchschnittlichen Compliance-Rate.

📖 *Die Compliance-Rate ist der Prozentsatz der zufriedenstellenden Kontrollen pro Stammregelwerk.*

Weitere Informationen zur Compliance-Rate finden Sie unter "Direkte Bewertung von Risiken", Seite 78

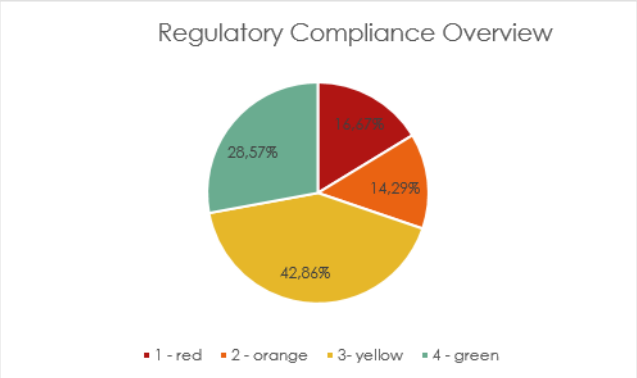
Globale Kontrollstufe

Tortendiagramm der Aufteilung der Regelwerke nach Compliance-Kategorie

📖 *Die Compliance-Rate ist der Prozentsatz der zufriedenstellenden Kontrollen pro Stammregelwerk.*

📖 *Eine Vorschrift oder ein Regelwerk stellt mehrere Richtlinien mit oder ohne Bedingungen auf, die von der Regierung im Rahmen eines*

Gesetzes, von einem Berufsverband in Form von Best Practices oder intern von einer Organisation festgelegt werden.



Um die Liste der Regelwerke eines Diagrammteils anzuzeigen, gehen Sie wie folgt vor:

- Klicken Sie auf das betreffende Teil.

Weitere Informationen zur Compliance-Rate finden Sie unter "Direkte Bewertung von Risiken", Seite 78

Bericht über die Verwaltung der Anbieter

☛ *Weitere Informationen zur Verwaltung der Anbieter finden Sie unter "IT-Anbieter verwalten", Seite 84.*

Kreuztabelle Anbieter nach Typ X Risikostufe

Pfad

Berichte > Verwaltung der IT-Anbieter > Anbieter nach Typ X Risikostufe

Parameter

N/A

Ergebnisse

Dieser Bericht präsentiert die Anzahl der Anbieter nach Risikostufe und Anbietertyp. Der Bericht bietet Zugriff auf die Liste der Anbieter.

Um auf die Anbieter zuzugreifen, gehen Sie wie folgt vor:

1. Klicken Sie auf die Zahl in den Zellen.
   Folgende Informationen werden für die einzelnen Anbieter angezeigt:
   - Anbietertyp
   - Name des Anbieters
   - Globale Risikobewertung
   - Gesamtbetrag der Einkäufe (Ende des vergangenen Jahres)
   - Rang

   ☛ *Weitere Informationen zur Eingabe dieser Informationen finden Sie unter "Merkmale der Anbieter", Seite 70.*

Beispiel

1. Matrix Vendor by Vendor Type X Risk Level

	Low	Medium	High
Services	0	0	0
Software	0	1	0
Software and Services	0	0	2
Total	0	0	0

Risikostufe Anbieter nach Geschäftssparte

Pfad

Berichte > Verwaltung der IT-Anbieter > Risikostufe Anbieter nach Geschäftssparte

Parameter

N/A

Ergebnisse

Dieser Bericht präsentiert die Anzahl der Anbieter nach Risikostufe und Geschäftssparte.

Eine Geschäftssparte ist eine hohe Klassierungsebene der wichtigsten Geschäftstätigkeiten eines Unternehmens. Sie entspricht zum Beispiel großen Produktsegmenten oder Distributionskanälen. Sie ermöglicht, Prozesse eines Unternehmens, organisatorische Einheiten oder Anwendungen für ein bestimmtes Produkt und/oder einen bestimmten Markt zu klassieren. Regelwerke bestimmter Industrien schreiben ihre eigenen Listen von Geschäftssparten vor.

In diesem Bericht können Sie nicht auf die Liste der Anbieter zugreifen.

Beispiel

1. Risk Level By Business Line

	Low	Medium	High
Banking	0	0	0
Agency Services	0	0	0
Asset Management	0	0	0
Commercial Banking	0	0	0
Corporate Finance	0	0	0
Payment and Settlement	0	0	0
Retail Banking	0	0	0
Retail Brokerage	0	0	0
Trading and Sales	0	0	0
Industry	0	2	1
Sale by partner	0	2	1
Sale in Agency	0	2	1
Sale on Internet	0	2	1
Sale to the professionals	0	2	1
WholeSales	0	0	0
Total	0	2	1

BERICHTE ÜBER DIE BEWERTUNGEN

☛ *Weitere Informationen zu den Bewertungen finden Sie unter "Bewertungen mit Fragebögen", Seite 87.*

Folgemaßnahmen - Sitzungen

Pfad

- Kampagnenmanagement > Folgemaßnahmen > Folgemaßnahmen der Sitzungen
- ab einer Bewertungssitzung

Um auf diesen Bericht ab einer Bewertungssitzung zuzugreifen, gehen Sie wie folgt vor:

1. Klicken Sie auf der Eigenschaftsseite einer Ausführungskampagne auf die Registerkarte **Sitzungen** und öffnen Sie die Eigenschaftsseite einer Bewertungssitzung.
2. Klicken Sie auf die Registerkarte **Reporting** und anschließend auf **Folgemaßnahmen**.

Parameter

- Bewertungssitzung

  🕮 *Eine Bewertungssitzung ist eine Bewertung, die zu einem bestimmten Zeitpunkt gestartet wird. Mit der Veröffentlichung der Bewertungssitzung soll ein Bewertungsfragebogen gesendet werden, in dem die Fragen gezielt an die Bewerter gerichtet werden.*

Ergebnis

In einer Zusammenfassung werden die allgemeinen Informationen zur aktuellen Bewertungssitzung angezeigt.

Dieser Bericht präsentiert mehrere Grafiken über den Fortschritt der Bewertungssitzung:

- Prozentsatz der ausgefüllten Fragebögen
- Aufteilung der Fragebögen nach Status
- Aufteilung der delegierten/nicht delegierten Fragebögen
- Aufteilung der Fragebögen nach Status, für jeden Beantworter
- Aufteilung der Fragebögen nach Status, für jedes bewertete Objekt

Sitzungsstatistiken

In diesem Bericht werden die Daten der Fragebögen einer Bewertungssitzung angezeigt. Mit dem Bericht lässt sich die Aufteilung der Antworten analysieren.

Pfad

Kampagnenmanagement > Folgemaßnahmen > Statistiken der Sitzungen

Parameter

Parameter	Hinweise
Kampagne	Obligatorisch
Sitzung	Obligatorisch

Ergebnis

Eine Baumstruktur wird angezeigt:

- in der Zeile: Fragen / Antworten und Beantworter
- in Spalten: für jede Frage/Antwort:
  - Anzahl der Beantworter
  - die Objekte, auf die sich die Antwort bezieht

  In dieser Baumstruktur wird angezeigt, wer was auf welche Frage geantwortet hat.

GLOSSAR

Aggregationsschema

Ein Aggregationsschema ist eine Folge von Schrien, mit denen die Ergebnisse einer Bewertung nach en geplanten Bewertungsregeln konsolidiert werden.

Aktion

Eine Aktion ist in einem Aktionsplan enthalten und stellt eine Umwandlung oder eine Bearbeitung in einer Organisation oder einem System dar.

Aktionsplan

Ein Aktionsplan besteht aus einer Reihe von Aktionen. Der Aktionsplan soll die Risiken oder Ereignisse reduzieren, die sich auf die Aktivitäten des Unternehmens negativ auswirken bzw. die Effizienz eines Prozesses oder einer Organisation verbessern können.

Anfälligkeit

Anfälligkeiten sind Fehler in der Kontrolle eines (IT) Assets, die sie auf eine Bedrohung anfällig machen und zu Mängeln beim Datenschutz, bei der Vollständigkeit oder der Verfügbarkeit dieses Assets führen können.

Anfälligkeitstyp

Anfälligkeitstypen gruppieren Anfälligkeiten nach verschiedenen Kategorien (Beispiel: Software, Organisationen, (geografischer) Standort usw.)

Anforderung

Eine Anforderung ist ein explizit ausgedrückter Bedarf oder eine Erwartung, die wie eine Einschränkung vorgeschrieben und im Rahmen eines Zertifikations-, Organisations- oder Modifikationsprojekts für das Informationssystem des Unternehmens erfüllt werden muss.

Anwendung

Eine Anwendung besteht aus Software-Komponenten, die im Rahmen der IT-Entwicklungen und Funktionalitäten für die Benutzer eine konsistente Einheit bilden.

Arbeitsschritt

Ein Arbeitsschritt ist eine Etappe eines Ablaufs, bei der eine Organisationseinheit der Organisation im Rahmen einer der Aktivitäten des Unternehmens handelt. Es kann sich hier um einen industriellen Arbeitsschritt handeln, wie „ein Teil fertigen", um einen logistischen Arbeitsschritt, wie „eine Lieferung annehmen", oder auch um eine Informationsverarbeitung, wie „eine Bestellung speichern". Ein Arbeitsschritt kann in elementare Aufgaben aufgeteilt werden.

Auswirkung

Eine Auswirkung beschreibt die Auswirkung des Risikos, wenn das Risiko auftritt.

Beantworter

Ein Beantworter ist eine Person in einem Unternehmen, die im Kontext einer Bewertung befragt wird. Diese Person muss den Bewertungsfragebogen ausfüllen und versenden.

Bedrohung

Bedrohungen sind externe oder interne Faktoren, die (IT) Assets des Unternehmens gefährden

Bedrohungstyp

Mit den Bedrohungstypen lassen sich die Bedrohungen nach verschiedenen Kategorien gruppieren (Beispiel: Körperschaden, Naturereignisse, technische Fehler usw.)

Benutzer

Ein Benutzer ist eine Person (oder eine Personengruppe) mit einem Login. Ein Benutzer verfügt über eine gewisse Anzahl von Zugriffsrechten für die Produktfunktionalitäten und Repositorys. Der Benutzer verfügt insbesondere in jedem Repository über einen eigenen Arbeitsbereich, mit dem er sich ab jedem beliebigen Arbeitsplatz einer gegebenen Umgebung verbinden kann. Der mit dem Benutzer während seiner Erstellung verknüpfte Code wird zum Erstellen verschiedener Dateinamen und insbesondere für sein Arbeitsverzeichnis verwendet. Standardmäßig können bei der Installation mit den Personen Administrator (Login: System) und Mega (Login: Mega) die Repositorys so administriert werden, dass neue Benutzer erstellt werden.

Bewertetes Merkmal

Das bewertete Merkmal legt fest, was bei einer Bewertung bewertet werden soll. Das Merkmal kann mit einer Metaclass verbunden werden, vor allem mit einem der MetaAttributs. Metaclass Risiko, MetaAttribut: Wahrscheinlichkeit.

Bewertung

Die Bewertung ist ein Mechanismus, mit dem einer identifizierten Population Fragebögen zugesendet werden, um (qualitative oder quantitative) Einschätzungen von identifizierten Objekten zu erhalten. Die Bewertung wird durch Werkzeuge für die Ergebnisanalyse ergänzt.

Bewertungsknoten

Ein Bewertungsknoten ist mit Werten verbunden, die ab den Antworten im Fragebogen des Beantworters für jedes bewertete Merkmal berechnet werden. Er wird entweder zum Zeitpunkt der Bereitstellung der Bewertungssitzung oder zum Zeitpunkt der Aggregation erstellt. Die bei der Bereitstellung erstellten Objekte gehören zur Sitzung und legen fest, welches Objekt von wem und in welchem Kontext bewertet werden soll.

Bewertungssitzung

Eine Bewertungssitzung ist eine Bewertung, die zu einem bestimmten Zeitpunkt gestartet wird. Mit der Veröffentlichung der Bewertungssitzung soll ein Bewertungsfragebogen gesendet werden, in dem die Fragen gezielt an die Bewerter gerichtet werden.

Bewertungsvorlage

Eine Bewertungsvorlage dient als Vorlage für die Erstellung von Bewertungskampagnen und Bewertungssitzungen. Die Bewertungsvorlage legt den Umfang der Bewertung fest, sowie die zu verwendende Fragebogenvorlage und eventuell die Aggregationsschemen, die für die Auslegung der globalen Ergebnisse verwendet werden.

Entität

Eine Entität kann eine unternehmensinterne oder -externe Entität sein: Eine interne Entität stellt ein Element der Organisation eines Unternehmens dar, wie beispielsweise eine Direktion, eine Abteilung oder einen Arbeitsplatz. Sie wird auf einer mehr oder weniger genauen Ebene definiert, je nachdem, wie präzise die Angaben über die Organisation sein müssen (siehe Organisationseinheitstyp). Beispiel: Finanzdirektion, Vertrieb, Marketingabteilung, Vertriebsmitarbeiter. Eine externe Organisationseinheit stellt eine Einrichtung dar, die Flüsse mit dem Unternehmen austauscht. Beispiel: Kunde, Lieferant, Administration.

Ereignis

Ein Ereignis ist ein Fakt einer internen oder externen Quelle, der sich auf die Organisation auswirkt. Er bildet das Grundelement für die Sammlung von Daten über ein Betriebsrisiko.

Fragebogen

In einem Fragebogen wird eine Liste von vordefinierten Fragen aufgeführt, die für einen Ereignistyp, eine Kontrolle, ein Dokument usw. gelten können.

Fragebogenvorlage

Eine Fragebogenvorlage stellt die Definition des Inhalts eines Fragebogens dar: Fragegruppe, Fragen, einmalige oder mehrere Antworten und mögliche Antworten. Die Fragebogenvorlage kann mit der Präsentation des Fragebogens verbunden werden, der die Anzeigeoptionen angibt. Die an die Bewerter gesendeten Fragebögen werden ab der Definition generiert, die in der Fragebogenvorlage geliefert wird.

Geschäftsfähigkeit

Eine Geschäftsfähigkeit ist eine Einheit zur Aufteilung der Bearbeitungen eines Informationssystems. Bei den Bearbeitungen kann es sich zum Beispiel um die Tätigkeit oder den Geschäftsbereich eines Unternehmens handeln.

Geschäftsprozess

Ein Geschäftsprozess stellt ein System dar, das Produkte oder Dienstleistungen an einen internen oder externen Kunden des Unternehmens oder Organisation liefert. Auf höherer Ebene definiert ein Geschäftsprozess eine Strukturierung und Kategorisierung des Geschäftsbereichs eines Unternehmens. Der Geschäftsprozess kann in weitere Prozesse unterteilt werden. Mit der Verbindung zu den organisatorischen Prozessen kann die reelle Implementierung des Geschäftsprozesses in der Organisation beschrieben werden. Ein Geschäftsprozess kann auch mit einer funktionalen Sicht detailliert werden.

Geschäftsrollen

Eine Geschäftsrolle definiert die Funktion einer Person im geschäftlichen Bereich. Eine Person kann mehrere Geschäftsrollen übernehmen. Geschäftsrollen werden nur verwendet, wenn die Option "Verwaltung der Zuweisung von Geschäftsrollen an Personen" aktiviert wurde. Ein Profil kann mit einer Geschäftsrolle verbunden sein. Wenn eine Person einer Geschäftsrolle zugewiesen wird, die mit einem Profil verknüpft ist, wird dieser Person indirekt ein Profil zugewiesen.

Geschäftssparte

Eine Geschäftssparte ist eine hohe Klassierungsebene der wichtigsten Geschäftstätigkeiten eines Unternehmens. Sie entspricht zum Beispiel großen Produktsegmenten oder Distributionskanälen. Sie ermöglicht, Prozesse eines Unternehmens, organisatorische Einheiten oder Anwendungen für ein bestimmtes Produkt und/oder einen bestimmten Markt zu klassieren. Regelwerke bestimmter Industrien schreiben ihre eigenen Listen von Geschäftssparten vor.

Geschwindigkeit

Die Geschwindigkeit stellt dar, wie schnell sich ein Risiko ab einem Asset bei einem Vorfall auf andere Assets ausweitet.

Gesellschaft

Eine Gesellschaft ist eine juristische Person.

Inhärentes Risiko

Ein Bruttorisiko bezeichnet ein Risiko für ein Unternehmen, wenn keine Maßnahmen getroffen werden, die Wahrscheinlichkeit oder Auswirkung dieses Risikos zu ändern. Es handelt sich um den Wert der Auswirkung, der vom Wert der Wahrscheinlichkeit produziert wurde, bevor Präventionsmaßnahmen oder Maßnahmen zur Risikominderung berücksichtigt werden.

IT Asset

Ein IT Asset ist ein Softwareartefakt (Beispiel: Anwendung, Softwaretechnologie) oder Hardwareartefakt (Beispiel: Standort, Server), das vom Unternehmen gehalten und im Rahmen seiner Geschäftstätigkeiten verwendet wird.

IT Asset (Instanz)

Eine Asset-Instanz ist ein spezifischer Typ des IT-Assets, der die Objekte einer Bereitstellung gruppiert (Softwareinstallation und bereitgestellte Technologie).

IT Asset (Typ)

Ein Asset-Typ ist eine spezifische Kategorie des IT-Assets, die Objekttypen (Anwendung, Softwaretechnologie usw.) gruppiert, im Gegensatz zu den bereitgestellten Objekten (Instanzen).

Kampagne

In einer Kampagne können mehrere Bewertungssitzungen gruppiert werden.

Kontextobjekt

Ein Kontextobjekt ist ein Objekt, in dessen Rahmen eine Bewertung vorgenommen wird. Zum Beispiel kann im Rahmen einer bereitgestellten Anwendung ein Risiko bewertet werden.

kontrollieren

Eine Kontrolle ist ein Mittel, ein oder mehrere Risiken unter Kontrolle zu haben, und sicherzustellen, dass eine gesetzliche, vorschriftsmäßige oder interne Anforderung des Unternehmens erfüllt wird.

Kontrollstufe

Die Kontrollstufe gibt an, inwieweit die bereitgestellten (kontrollierten) Kontrollelemente für die Bewertung eines Risikos effizient sind.

Kontrolltyp

Mit einem Kontrolltyp lassen sich die Kontrollen klassieren, die im Unternehmen entsprechend des Standards bzw. Normen der betreffenden Sektoren oder Vorschriften/Reglementierungen (Cobit usw.) implementiert sind.

Lenkungsdatum

Ein Lenkungsdatum ist ein Datum, das in einem Lenkungskalender festgelegt wird und an dem der verantwortlichen Person eines Elements eine Erinnerung gesendet wird. Ein Anfangsdatum, ein Erinnerungsdatum oder ein Termin (Enddatum).

Lenkungskalender

Mit dem Lenkungskalender können wiederholte Aktionen zu vordefinierten Terminen durchgeführt werden. Man kann den Kalender zum Beispiel verwenden, um Erinnerungen an die Person zu senden, die für einen Aktionsplan verantwortlich ist, damit sie den Fortschritt angibt, der bei diesem Aktionsplan erzielt wurde. Man kann einen Lenkungskalender auch verwenden, um den Start von Bewertungssitzungen zu regelmäßigen Terminen auszulösen ...

Person

Eine Person wird mit ihrem Namen und ihrer E-Mail-Adresse definiert. Um auf **MEGA** zuzugreifen, kann eine Person auf das Produkt zugreifen, sobald sie eine ID (Login) zur Verbindung erhalten hat. Auch eine oder mehrere Geschäftsrollen kann der Person zugewiesen werden. Diese Personenliste kann zum Beispiel von einem LDAP-Server stammen.

Profil

Ein Profil definiert, was eine Person sehen bzw. in den Tools machen darf oder nicht und wie er es sieht und machen darf. In einem Profil werden die Optionen, die Zugriffsrechte für Repositorys und Produkte und die Rechte für den Schreibschutz bzw. zum Einlesen der Objekte definiert. Alle Benutzer mit demselben Profil haben dieselben Optionen und Rechte.

Risiko

Ein Risiko ist eine mehr oder weniger wahrscheinliche Gefahr, der einer Organisation ausgesetzt ist.

Risikofaktor

Ein Risikofaktor ist ein Element, das zum Auftreten eines Risikos beiträgt oder ein Risiko auslöst. Für verschiedene Risiken kann ein und derselbe Risikofaktor verantwortlich sein. Beispiele: Die Verwendung eines gefährlichen chemischen Produkts, eine komplexe Anwendung, die Größe eines Projekts, die Anzahl der Mitwirkenden, eine neue Technik, mangelnde Qualitätssicherung, mangelnde Sorgfalt bei der Festlegung der Anforderungen usw.

Risikofolge

Die Folge eines Risikos kann positiv oder negativ sein. Sie wird mit einem Typ verbunden, mit dem sich die Folge charakterisieren lässt. Beispiel: Bild, Umgebung, Angestellte.

Risikoszenario

Ein IT-Risikoszenario ist die Beschreibung eines IT Ereignisses, das sich auf die Geschäftstätigkeit eines Unternehmens auswirken kann, sofern es eintritt.

Risikotyp

Ein Risikotyp definiert die Typologie eines normalisierten Risikos im Rahmen einer Organisation.

Softwareinstallation

Eine Softwareinstallation stellt die Bereitstellung einer Anwendung dar, die an einem bestimmten Standort verwendet werden soll.

Softwaretechnologie

Eine Softwaretechnologie ist eine Grundkomponente, die für Geschäftsanwendungen notwendig ist.

Die Softwaretechnologien umfassen die gesamte Basic Software: Anwendungsserver, Mail Server, Softwarekomponenten für die Darstellung, Eingabe, Ablage, gemeinsame Nutzung der Geschäftsdaten, Betriebssysteme, Middleware, Navigatoren usw.

Typ eines IT Assets

Ein Asset-Typ ist eine Asset-Kategorie, die Objekttypen (Anwendung, Software, Technologie) gruppiert, im Gegensatz zu den bereitgestellten Objekten, die Instanzen genannt werden.

Vorgang

Ein Vorfall ist ein Fakt einer internen oder externen Quelle, der sich auf die Organisation auswirkt. Er bildet das Grundelement für die Sammlung von Daten über ein Betriebsrisiko.

Vorschrift oder Regelwerk

Eine Vorschrift oder ein Regelwerk stellt mehrere Richtlinien mit oder ohne Bedingungen auf, die von der Regierung im Rahmen eines Gesetzes, von einem Berufsverband in Form von Best Practices oder intern von einer Organisation festgelegt werden.

Wahrscheinlichkeit

Die Wahrscheinlichkeit, dass das Risiko auftritt.

Zentrales Risiko

Ein zentrales Risiko ist ein Risiko, das in einem Diagramm über ein Risikoszenario mit mindestens einer Ursache und eventuell einer oder mehreren Folgen verbunden ist.

Ziel

Ein Ziel ist ein Ergebnis, das erreicht werden soll, oder das angestrebte Resultat eines Prozesses oder eines Arbeitsschritts. Mit einem Ziel können die Punkte hervorgehoben werden, die für diesen Prozess oder diesen Arbeitsschritt verbessert werden sollen.

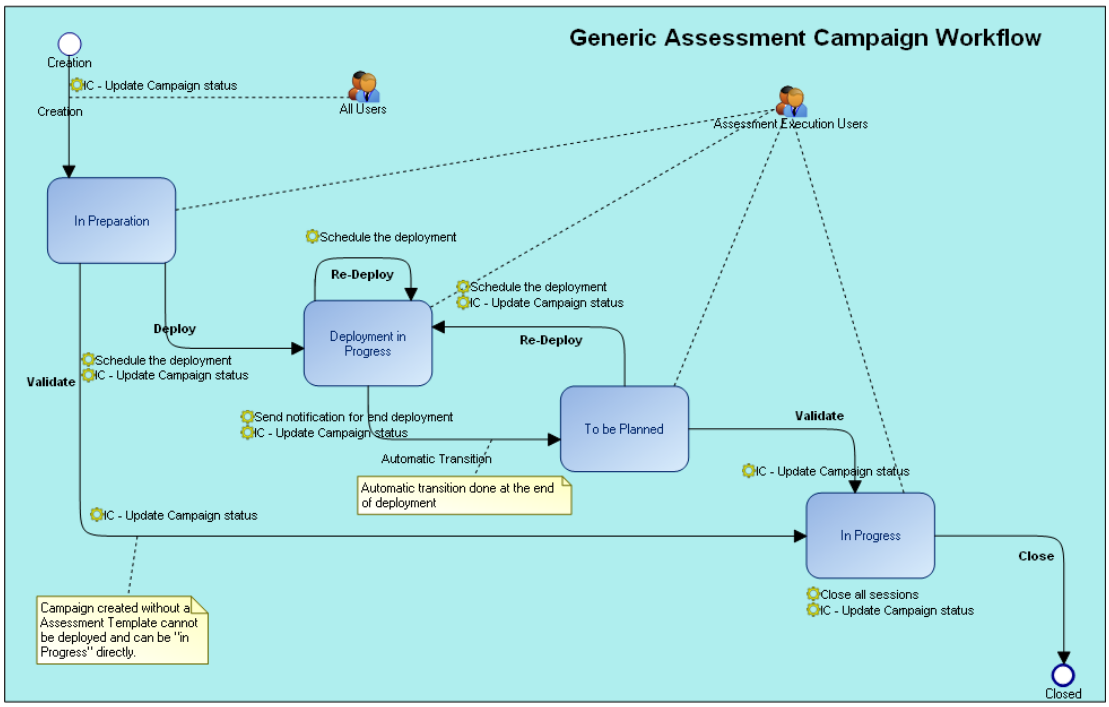
ANHANG - WORKFLOWS

✓ "Workflow von Bewertungen", Seite 158
✓ "Workflows der Aktionspläne", Seite 161

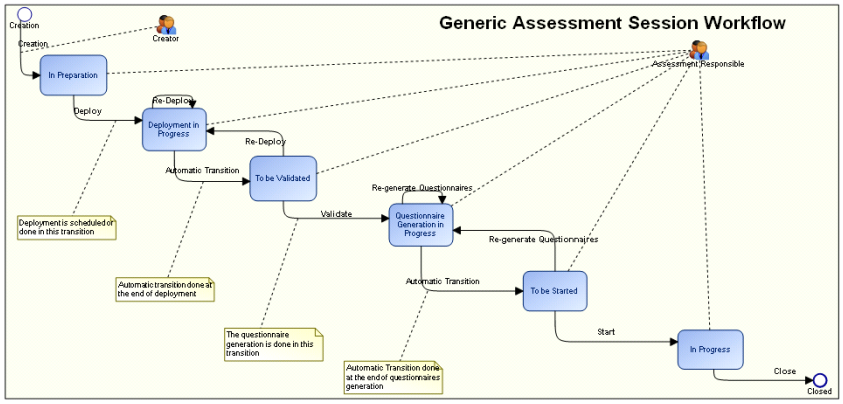
WORKFLOW VON BEWERTUNGEN

☛ *Ein Beispiel für den möglichen Workflow-Sequenzfluss finden Sie unter "Kampagne und Bewertungssitzungen starten", Seite 89*

Generischer Workflow einer Bewertungskampagne



Generischer Workflow einer Bewertungssitzung



Generischer Workflow der Fragebögen

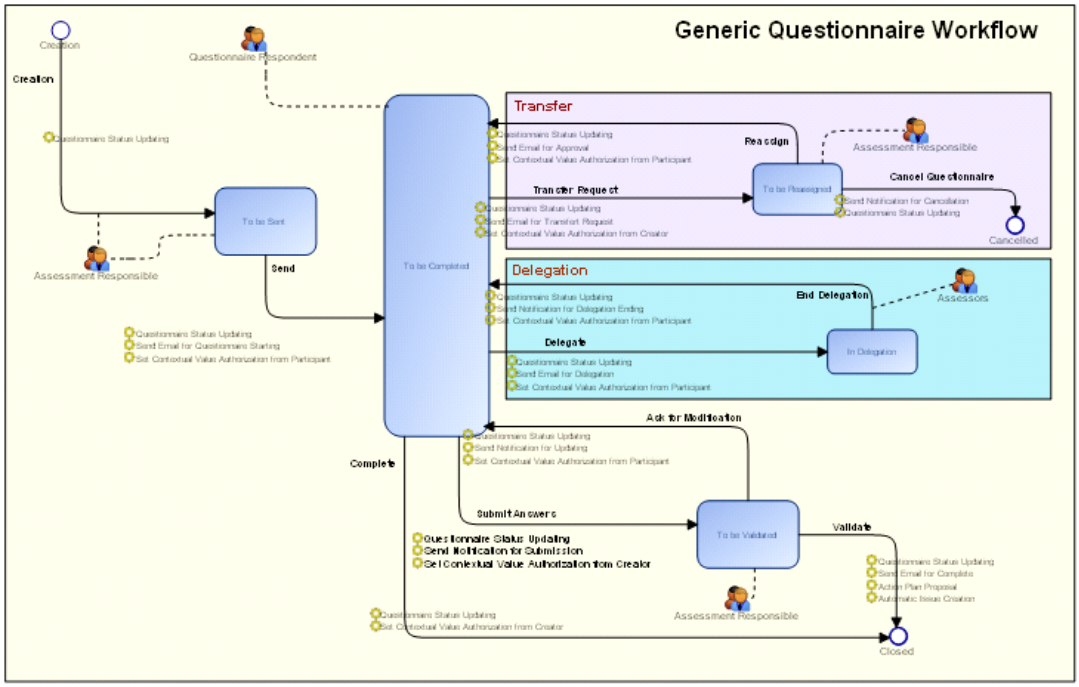
Die Fragebögen sind mit einer Bewertungssitzung verbunden und enthalten eine oder mehrere Fragen.

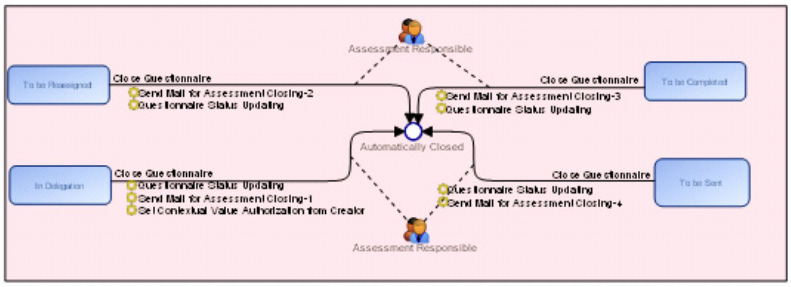
Die Fragebögen werden abhängig vom definierten Umfang generiert, der in der Bewertungssitzung, dem Bewertungsmodell und dem Bewertungsfragebogen definiert wird.

Sie werden automatisch an die Beantworter gesendet, wenn die Bewertungssitzung gestartet wird.

Ein Beantworter kann den Fragebogen an den Verantwortlichen der Bewertung senden, wen er nicht der richtige Empfänger ist. Er kann ihn auch an einen anderen Beantworter delegieren, wenn der Fragebogen ganz oder teilweise delegiert werden kann.

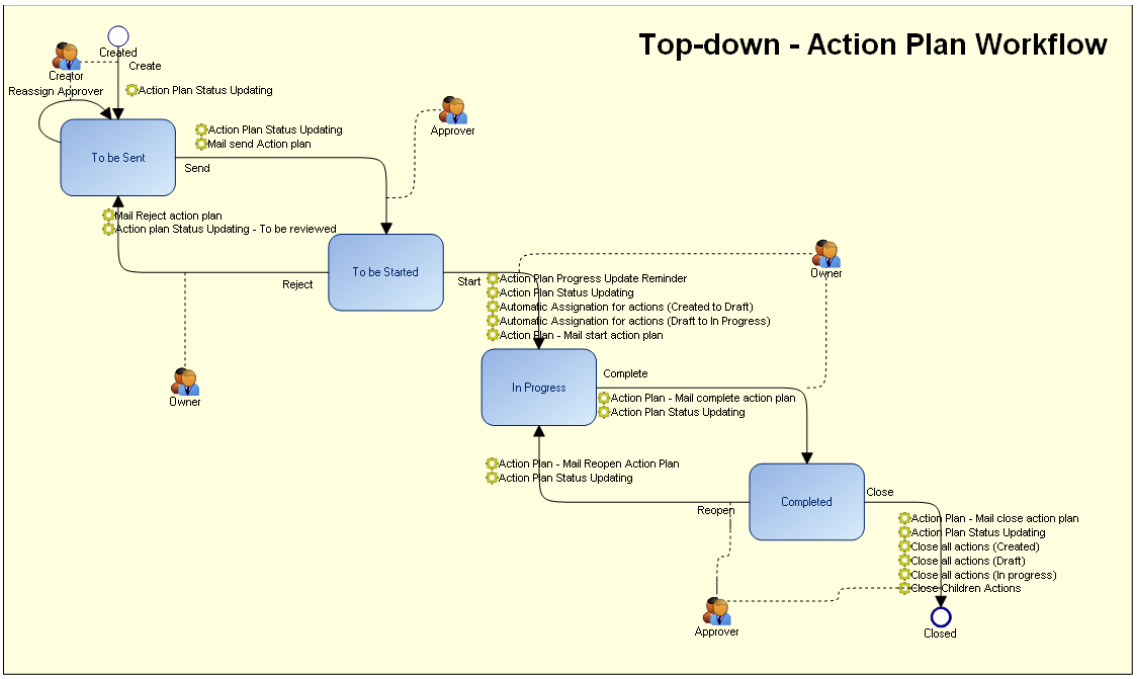
Der Beantworter schließt den Fragebogen, wenn er ihn ausgefüllt hat, sollte der Workflow keine Freigabe vorsehen. Er kann ihn zur Freigabe auch an den Verantwortlichen der Sitzung senden.



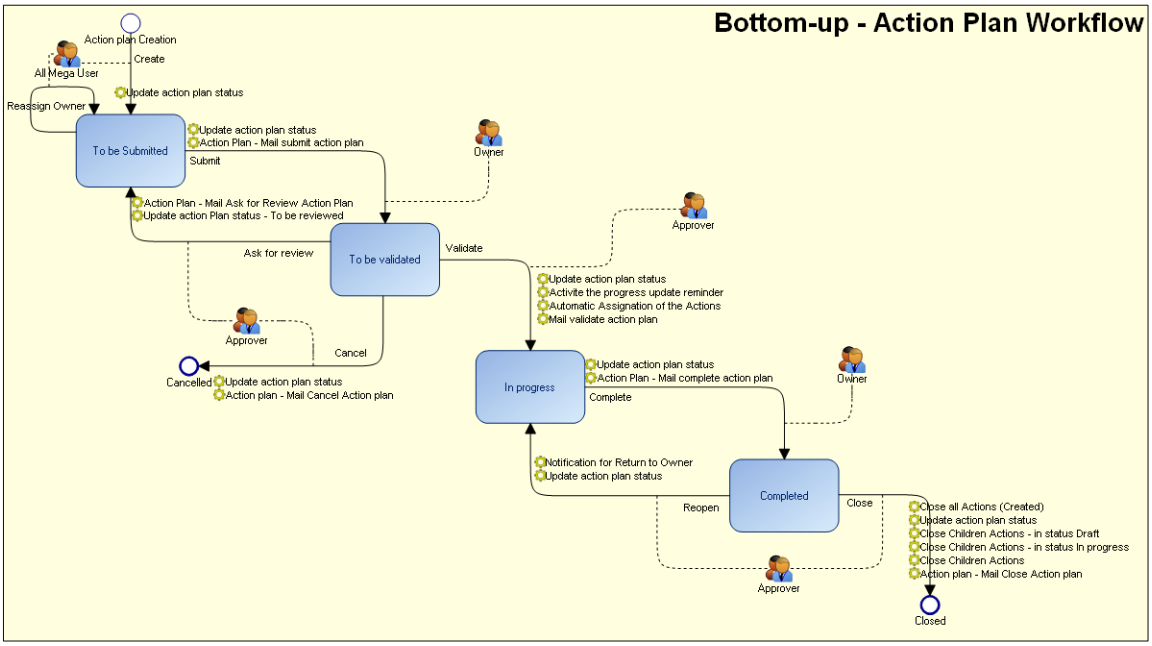


WORKFLOWS DER AKTIONSPLÄNE

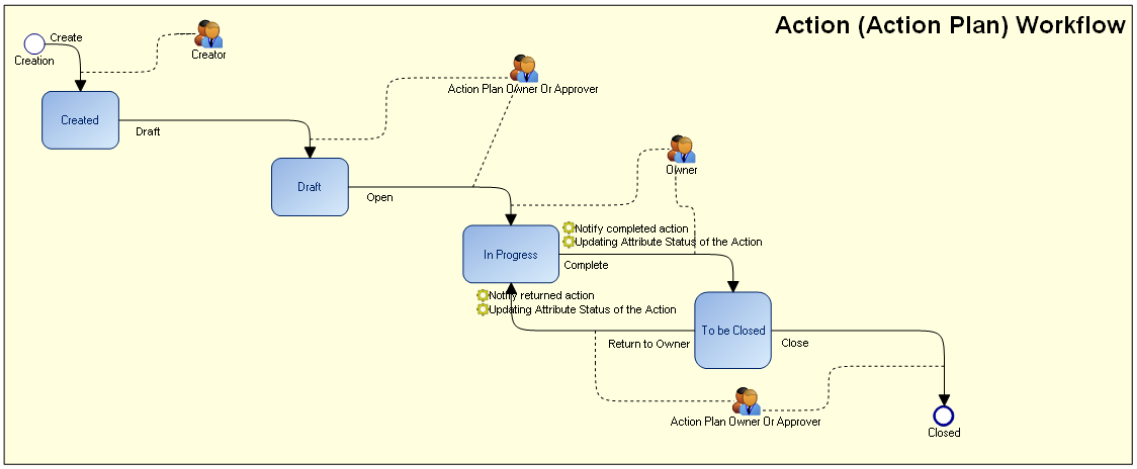
Workflow des Aktionsplans "Top-down"

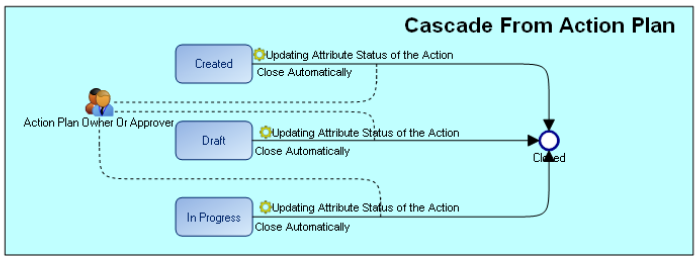


Workflow des Aktionsplans "Bottom-up"



Workflow einer Aktion





INDEX

A

Aggregation
  Starten 138
Aktionsplan
  Erstellen 113
  Fortschritt 117
  Lenkungskalender 114
Akzeptieren
  Risiko 110
Analyse
  Risiko 38
Anbieter
  Bestand 70
  Bewerten 85
    Risiko 70
  Identifizieren 84
  Kosten 84
  Merkmale 70
  Verwalten 84
  Zugreifen 70
Änderung
  Antworten
    Fragebögen 105
Anfälligkeit
  Beispiel 61
  Bestand 61
  Datum
    Änderung 63
  Erstellen 59
  Positionieren 72
  Quelle 63
  Score 63, 64
  Status 63
  Typ 63
    Erstellen 62
  Umfang 64
  Widget 132
Anfälligkeitstyp
  Beispiel 61
Anfällilgkeit
  Aufrufen 62
Anforderung
  Definieren 81
  Priorität 48
  Umfang 46
  Vorfall 47
  Vorschrift 45
Anschrift
  Anbieter 70
Anwendung 59
  Beschreiben 57
  Code 57
  Funktionaler Umfang 57
  Nachrichtenfluss 59
  Verantwortung 58
Anwendungseigentümer
  IT RM 25
Anzeigen
  Fragebogen 100
Arbeitsplatz
  Definition 154
Asset
  Anfällig 64
  Bereitgestellt 56
Aufteilen
  Sitzungen 95
Aufteilung
  Kontrollen 136
Aufwand
  Kontotyp 49
Ausfüllen
  Fragebogen 103

Auswirkung 66

B

Beantworter
Angeben 95, 99
Bearbeitung
Risiko
Modus 110
Bedrohung
Beispiel 61
Bestand 61
Typ 62
Erstellen 62
Zugreifen 61
Beitragsleistender
Anforderung 47
Bereitgestellt
IT Asset 56
Bereitstellen
Bewertungskampagne 94
Bereitstellung
Anwendung 59
Bericht
Bewertungen 146
Identifizierung der Kontrollen 135
IT-Assets 126
IT-Compliance 135
Risikoidentifizierung 124
Risikostufe 126
Ursache 76
Verwaltung der Anbieter 144
Zugreifen 122
Bestand
IT 56
Bewerten
Anbieter 85
Risiko
Experte 78, 82
Bewertetes Merkmal 66
Bewertung
Etappen 88
Fragebogen 87
Prinzip 88
Umfang 92
Vorbereiten 88
IT RM 68
Workflows 157
Bewertungskampagne
Beantworter 95
Bereitstellen 94
Erstellen 91
Freigeben 97
Planen 95
Zugreifen 91
Bewertungsknoten 94
Bewertungssitzung
Beantworter 99
Bereitstellen 98
Erstellen 92
Freigeben 100
Schließen 108
Starten 102
Statistiken 146
Umfang 99
Bewertungsvorlage 91
Kontrolle
IT RM 83
Risiko
IT RM 79
Bottom-up
Aktionsplan 116
Büroautomation 60

C

COBIT
Kontrolle 41
Compliance
IT 80
Rate 142
CVSS
Bewertung 64

D

Dashboard
Zugreifen 122
Datenbank
Beschreibung 52
Datum
Veröffentlichung
Anfälligkeit 63
Diagramm
Risikoszenario 74
Durchführungsverantwortlicher
RACI 53

E

Eigentümer
  Lokal
    Anwendung 58
Einschränkung
  Element 47
Empfänger
  Fehler 103
Entität 32
  Baumstruktur 32
  Erstellen 33
  Umgebung 33
Erfolg
  Faktor
    Aktionsplan 115
Ergebnis
  Sitzung 105
Etappen
  Bewertung 88

F

Fakturierung
  Anbieter 70
Fehler
  Empfänger 103
Finanzen
  Konto 49
Folge
  Risiko
    Szenario 75
Folgemaßnahmen
  Sitzungen 146
Folgen
  Risiko 39
Fortschritt
  Aktionsplan 117
  Fragebögen 105
Fragebogen
  Ändern
    Antworten 105
  Ausfüllen 103
  Fortschritt 105
  Freigeben 105
  Generieren 100
  Gesendet 105
  Neu zuweisen 106
  Senden 102
  Übertragung 103
  Zugreifen 103
Framework
  Importieren 19
Freigabeverantwortlicher
  Aktionsplan 114
Freigeben
  Bewertungskampagne 97
  Bewertungssitzung 100
  Fragebogen 105
Funktionaler Administrator
  IT-Risiken 24
Funktionaler Umfang
  Anwendung 57

G

Generieren
  Fragebögen 101
Geschäftsdaten
  Nachrichtenfluss 59
Geschäftsfähigkeit
  Anwendungsumfang 58
Geschäftsprozess
  Anwendungsumfang 57
Geschäftsrolle
  IT RM 24
  Rechte 25
Geschäftssparte
  Anwendungsumfang 57
  Organisation 34
Geschwindigkeit 66
Gewinne
  Konto 49
Grundvoraussetzungen
  Bewertung
    IT RM 68

H

Heatmap
  Anwendungen 129
  Risiken 127

I

Identifizieren
  Kontrollen
    Bericht 82, 135
  Risiken
    Bericht 124
Importieren
  Framework 19
Informiert
  RACI 53
Inhärent
  Risiko
    Gewichtet 66
Inhärentes Risiko
  Gewichtet 66
Installation
  Software 56
    Zugreifen 59
Instanz
  IT Asset 56
Interne Vorschriften 43
IT Asset
  Instanz 56
  Typ 56
IT RM
  Geschäftsrolle 24
IT RM Manager 24

K

Kennwort 20
Konsultiert
  RACI 53
Konto
  Finanzen 49
  Status 49
  Typ 49
Kontotyp 49
Kontrolle
  Ausführungsmethode 40
  Merkmale 41
  Status 40
  Typ 41
  Umfang der Anwendungen 81
  Zufriedenstellend 83
  Zugreifen 68
Kontrollstufe 83
  Global 142
Kosten
  Anbieter 84

L

Lenkungskalender
  Aktionsplan 114
Local IT Risk Manager 58

M

Meilenstein
  Aktionsplan 115
Merkmal
  Bewertet 93
Middleware 57
Mindern
  Risiko 110

N

Nachrichtenfluss
  Anwendung 59
  Geschäftsdaten 59
Neu generieren
  Fragebögen 101
Neu zuweisen
  Fragebogen 106

O

Organisation
  Geschäftssparte 34
Organisatorischer Prozess
  Umgebung 30

P

Planen
- Bewertungskampagne 95
- Bewertungssitzungen 94

Priorität
- Aktionsplan 114

Produkt
- Erstellen 48
- Kontotyp 49
- Vorfall 48

Prozess
- Einführung 30
- Typ 30

R

RACI
- Durchführungsverantwortlicher 53
- Informiert 53
- Konsultiert 53
- Rechenschaftspflichtig 53
- Risiko 40, 41

Rate
- Compliance 142

Rechenschaftspflichtig
- RACI 53

Rechte 25

Risiko
- Analyse 38
- Eigenschaften 36, 40
- Folge 75
- Identifizieren 73
- Identifizierungsmodus 36
- Inhärent 66
- Kontrolle
  - *Präventiv* 111
- Positionieren 73
- Risikofaktor 39
- Stufe 111
- Szenario 74
- Umfang 67
- Ursache 75
- Zugreifen 66

Risikofaktor
- Risiko 39

Risikostufe
- Anbieter 145
- Bericht 126

Risikoszenario 74

Risikotyp
- Erstellen 39

S

Score
- Anfälligkeit 64

Senden
- Fragebogen 102

Sitzung
- Folgemaßnahme 146

Softwareprogrammpaket 57

Standort
- Bereitgestellte Anwendungen 59

Statistiken
- Sitzungen 146

Status
- Konto 49
- Kontrolle 40

Stufe
- Risiko 111

System 57

T

Technologie
- Angeben 59
- Angeboten 70
- Bereitgestellt 56
- Beschreiben 59
- Typ 60
- Zugreifen 59

Top-down
- Aktionsplan 117

Typ
- Anfälligkeit
  - *Erstellen* 62
- Bedrohung
  - *Erstellen* 62
- IT Asset 56
- Kontrolle 41
- Technologie 60

U

Übertragen
  Risiko 110
Übertragung
  Fragebogen 103
Umfang
  Aktionsplan 115
  Bewertung 92
  Definieren 95
Umgebung
  Analyse 27
  Arbeit 21
  Entität 33
  Organisatorischer Prozess 30
  RACI 53
Ursache
  Bericht 76
  Risiko 75
  Risikoszenario 75

V

Verantwortung
  Anwendung 58
  RACI 53
Verarbeitung 111
  Risikostufe 111
Verluste
  Konto 49
Veröffentlichung
  Datum
    Anfälligkeit 63
Versicherung
  Risiko 111
Vorfall
  Anforderung 47
  Produkt 48
Vorschau
  Fragebogen 100
Vorschrift
  Anforderung 45
  Merkmale 43
Vorschriften 43
  Liste 43

W

Wahrscheinlichkeit 66
Widget
  Anfälligkeit 132
  Risiken 130
  Zugreifen 122
Workflows
  Bewertungen 157

Z

Zentral
  Risiko 75
Zentrales Risiko 75
Zufriedenstellend
  Kontrolle 83
Zulieferer
  Risiko 110
Zuweisung
  Neu 106
  Person
    Neu zuweisen 107